

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al.*,

Plaintiff,

v.

BRAD RAFFENSPERGER, *et al.*,

Defendants.

CIVIL ACTION NO.
1:17-cv-2989-AT

OPINION AND ORDER

I. Introduction

This election case is currently before the Court on the Defendants' Motions for Summary Judgment. [Docs. 1567, 1568, 1571].

Elections are contentious matters. So too are election cases. *See Bush v. Gore*, 531 U.S. 98 (2000). But the central issue in this case is not about partisan advantage, nor is it about how the winner of any specific election should be selected or why a particular group of voters or candidates have allegedly been favored over others, and it does not involve allegations of fraud. *Cf. Jacobson v. Fla. Sec'y of State*, 974 F.3d 1236 (11th Cir. 2020); *Wood v. Raffensperger*, 981 F.3d 1307 (11th Cir. 2020). Instead, this case focuses on whether Georgia's statewide electronic voting system,¹ as currently designed and implemented, suffers from major

¹ The State's election system equipment is uniformly used throughout Georgia for in-person voting in all elections, except when a select number of jurisdictions hold elections for a small number of

cybersecurity deficiencies that unconstitutionally burden Plaintiffs' First and Fourteenth Amendment rights and capacity to cast effective votes that are accurately counted.²

Since its inception, this election case has gone through multiple stages of evolution. Plaintiffs have raised challenges to both the original, critically outdated Direct Recording Electronic ("DRE") voting system and the current Dominion Ballot Marking Device ("BMD") system that replaced the DRE system several years into the case, starting in 2020. A plethora of new factual and legal developments emerged along the way, topped off by the breach of the Coffee County election system in early 2021. This breach and the copying and sharing of election system software and voting data to actors and entities inside and outside of the state, as well as through the internet, bear serious ramifications for the future vulnerability of the State's election system as a whole. Plaintiffs initially discovered this breach in 2021 and, thereafter in 2022, conducted a series of depositions of individuals involved in the breach, some of whom were indicted in the pending RICO criminal case in Fulton County Superior Court. *See Georgia v. Trump et al.*, 23SC188947 (Fulton Cty. Super. Ct. Aug. 14, 2023).

local offices in off election cycle years. O.C.G.A. § 21-2-300. Absentee ballots are processed and tallied on county electronic scanners, which are also provided by the State.

² The Court notes that the record evidence does not suggest that the Plaintiffs are conspiracy theorists of any variety. Indeed, some of the nation's leading cybersecurity experts and computer scientists have provided testimony and affidavits on behalf of Plaintiffs' case in the long course of this litigation.

This case's broad evidentiary scope can be daunting. To assist the reader's review of the Order, the Court has started by first providing a cast of many of the key individuals and experts who, in the last few years, have played a role in this case as well as a glossary of specialized terms and abbreviations. The Court then proceeds to provide information necessary to give context for a range of relevant topics, including, among others:

- the use of computerized electronic voting systems in Georgia and the history of the cybersecurity and voting issues raised by Plaintiffs in their series of legal challenges, as previously addressed by this Court;
- the cybersecurity and reliability issues surrounding the use of the relevant electronic voting systems and the auditing of such systems and voting results;
- the cybersecurity experts' evaluations and testimony regarding the State's voting systems and exposure to breaches, especially in the absence of timely, needed software patches and the implementation of other cybersecurity protective measures;
- the Department of Homeland Security's Cybersecurity & Infrastructure Agency's ("CISA") review of the Dominion ImageCast X system and software (currently used in Georgia) and CISA's issuance of a national advisory notice on June 3, 2022 recommending that jurisdictions using this particular Dominion software and related technology implement specific measures to limit unauthorized access or manipulation of voting systems;
- the serious security issues and long-term ramifications surrounding the breach of the Coffee County election system and unauthorized access to the State Dominion voting software and election data, and the resulting impact on future voting security;³

³ Issues regarding the State Defendants' delayed and incomplete review of the Coffee County breach are addressed in Section IV.E.4.f of this Order.

- Defendants’ principal defense that Plaintiffs lack standing to assert the constitutional claims raised in this case and, on the other side, the grounds Plaintiffs rely on to establish their legal standing to pursue their claims in this case — grounds including the alleged severe burden placed on their capacity to cast an effective and reliable vote by Defendants’ handling of the election system;
- The Court’s legal and evidentiary analysis of the issues in dispute raised by the Defendants’ pending Motions for Summary Judgment.

As these evidentiary and legal issues are complex and interwoven, review of this Order takes patience. Ultimately, the Court concludes that there are material facts in dispute presented in the record that preclude its grant of the State Defendants’ Motions for Summary Judgment on the primary claims. [Docs. 1567, 1568.] The Court will resolve these material factual disputes and related legal issues based on the evidence presented at a bench trial to begin on January 9, 2024. That said, the Court finds that several distinct requests for relief advanced solely by the Coalition Plaintiffs are largely outside the scope of this case, as discussed in Section V.D. of this Order. The Court also concludes that Fulton County’s Motion for Summary Judgment [Doc. 1571] should be granted based on the County’s lack of direct authority over the voting system matters in dispute here.

To be clear from the start, the Court does not have the legal authority to grant the broadest relief that Plaintiffs request in this case without directly infringing on the state legislature’s vested power to enact legislation. Even if Plaintiffs prevail on their substantive claims, the Court cannot order the Georgia legislature to pass legislation creating a paper ballot voting system or judicially impose a statewide

paper ballot system as injunctive relief in this case. Quite simply, the Court has the legal authority to identify constitutional deficiencies with the existing voting system, but it does not have the power to *prescribe or mandate* new voting systems (i.e., a paper ballot system) to replace the current, legislatively enacted system. *See Burdick v. Takushi*, 504 U.S. 428, 433–34 (1992); *Wood v. Raffensperger*, 501 F. Supp. 3d 1310, 1327–28 (N.D. Ga. 2020), *aff'd*, 981 F.3d 1307 (11th Cir. 2020).

That said, as the Eleventh Circuit previously recognized in this case, “suits challenging election procedures [or policies] are routine,” and there are critical issues raised in this case that do not “present a political question beyond this Court’s reach.” *Curling v. Raffensperger*, 50 F.4th 1114, 1121 n.3 (11th Cir. 2022). Still, Plaintiffs carry a heavy burden to establish a constitutional violation connected to Georgia’s BMD electronic voting system, whether in the manner in which the State Defendants have implemented the voting system — i.e., that it imposes serious security voting risks and burdens impacting Plaintiffs’ voting rights — or otherwise. If Plaintiffs prevail at trial on one or more of their claims, there are pragmatic, sound remedial policy measures that could be ordered or agreed upon by the parties, such as (1) providing for the use of printed ballots for vote counting *without* the use of QR codes, (2) administering a broader scope and number of election audits to address vote count accuracy and other related issues, and (3) implementing other essential cybersecurity measures and policies recommended by the nation’s leading cybersecurity experts and firms, including the Department of Homeland Security’s CISA.

As the Court has consistently advised the parties, it is in the public interest for them to seriously engage in the hard work of attempting to reach a consensual resolution regarding those voting system remedial measures that the State could implement and that the legislature could authorize funding for in the year ahead. The Court cannot wave a magic wand in this case to address the varied challenges to our democracy and election system in recent years, including those presented in this case. But reasonable, timely discussion and compromise in this case, coupled with prompt, informed legislative action, might certainly make a difference that benefits the parties and the public. For now, though, the Court must proceed with trial starting on January 7, 2023.

II. Legal Standard

The Court may grant summary judgment only if the record shows “that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). A factual issue is genuine if there is sufficient evidence for a reasonable jury to return a verdict in favor of the non-moving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A factual issue is material if resolving the factual issue might change the suit’s outcome under the governing law. *Id.* The motion should be granted only if no rational fact finder could return a verdict in favor of the non-moving party. *Id.* at 249.

When ruling on the motion, the Court must view all the evidence in the record in the light most favorable to the non-moving party and resolve all factual

disputes in the non-moving party's favor. See *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000). The moving party need not positively disprove the opponent's case; rather, the moving party must establish the lack of evidentiary support for the non-moving party's position. See *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986). If the moving party meets this initial burden, in order to survive summary judgment, the non-moving party must then present competent evidence beyond the pleadings to show that there is a genuine issue for trial. *Id.* at 324–26. The essential question is “whether the evidence presents a sufficient disagreement to require submission to a jury [or trial judge] or whether it is so one-sided that one party must prevail as a matter of law.” *Anderson*, 477 U.S. at 251–52.

III. Cast of Characters and Glossary of Terms

Before the Court plunges into the factual background of this matter, it provides for the reader's reference a “Cast of Characters” that includes the various parties, entities, and other individuals who play a significant role in this case. The Court lists only the individuals and entities that are specifically mentioned in this Order.⁴

CAST OF CHARACTERS⁵

⁴ When citing to depositions or transcripts, the Court references the official deposition or transcript page number. When citing to prior orders issued by the Court or the parties' briefs, the Court uses the page number indicated at the bottom of the order or brief. Where a document or exhibit includes no clear page number identification, the Court refers to the designated ECF page number and indicates this reference by stating in the citation “at ECF [page number].”

⁵ In providing this background information, the Court does not include record citations to identify the primary individuals but does include citations to identify experts and secondary players.

Plaintiffs and Their Representatives

Curling Plaintiffs	The Curling Plaintiffs include Donna Curling, Donna Price, and Jeffrey Schoenberg.
Coalition Plaintiffs	The Coalition Plaintiffs include the Coalition for Good Governance (“CGG”), Laura Digges, William Digges, Ricardo Davis, and Megan Missett.
The Coalition for Good Governance (“CGG”)	CGG is a non-profit, non-partisan corporation registered under the law of Colorado that concentrates on issues of election security and transparency.
Marilyn Marks	Ms. Marks is the executive director of CGG. However, she is not an individual Plaintiff in this litigation.

Defendants

State Defendants	The State Defendants include the Secretary of State of Georgia in his official capacity and members of the Georgia State Election Board, also in their official capacities.
Fulton County Defendants	The Fulton County Defendants include members of the Fulton County Board of Registration and Elections in their official capacities.

Officials of the Georgia Secretary of State’s Office

Brad Raffensperger	Mr. Raffensperger is Georgia’s Secretary of State.
Gabriel Sterling	Mr. Sterling is the Chief Operations Officer for Georgia’s Secretary of State.
Merritt Beaver	Mr. Beaver is the Chief Information Officer for Georgia’s Secretary of State.
Chris Harvey	Mr. Harvey is the former Director of Elections for the Georgia Secretary of State (succeeded by Blake Evans). He was previously the Chief Investigator and Deputy Inspector General for the Georgia Secretary of State.
Michael Barnes	Mr. Barnes was the Director of the Center for Election Services (“CES”) maintained by

There are also additional experts and individuals who have appeared and given testimony during the long course of this litigation who are not identified in this list of characters.

	Kennesaw State University (“KSU”) and reported to the Executive Director, Merle King. After the State closed the KSU CES, Mr. Barnes was transferred in January 2018 to perform the same role in the Secretary of State’s Office. (9/17/2018 PI Order, Doc. 309 at 35.)
Ryan Germany	Mr. Germany is the former general counsel for the Georgia Secretary of State. Charlene McGowan replaced Mr. Germany on February 25, 2023.

Experts

Plaintiffs’ Experts

Dr. J. Alex Halderman	Dr. Halderman is a Professor of Computer Science & Engineering at the University of Michigan and Director of the University’s Center for Computer Security and Society. He is a nationally recognized expert in the fields of cybersecurity and computer science in the context of elections. He has testified in numerous forums regarding cybersecurity, including at the United States Senate Select Committee on Intelligence in connection with its 2017 investigation of Russian election hacking. He is one of the Curling Plaintiffs’ experts. (Pls.’ Statement of Additional Facts, Doc. 1637 ¶ 134.)
Dr. Philip Stark	Dr. Stark is a Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley; a faculty member in the Graduate Program in Computational Data Science and Engineering; a co-investigator at the Berkeley Institute for Data Science; and was previously the Chair of the Department of Statistics and Director of the Statistical Computing Facility. (<i>See generally</i> Sept. 9, 2018 Decl. of Philip B. Stark, Doc. 296.) He is a coauthor on papers on end-to-end cryptographically verifiable voting systems. Dr. Stark has consulted for many government agencies and currently serves on the Advisory Board of the U.S. Election Assistance Commission and its cybersecurity subcommittee. In addition to testifying as an expert in statistics in both federal and state courts, Dr. Stark has

	testified before a host of other federal and state legislative committees about election integrity, voting equipment, and election audits. Dr. Stark’s statistical “risk-limiting audits” approach to auditing elections has been incorporated into statutes in several states and in some respects in Georgia’s new Election Code. (<i>Id.</i>)
Kevin Skoglund	Mr. Skoglund is a cybersecurity expert and consultant. He serves on the National Institute of Science and Technology Voting System Cybersecurity Working Group, which is an advisory group to the U.S. Election Assistance Commission. He is one of the Coalition Plaintiffs’ experts. (Dec. 12, 2022 Dep. of Kevin Skoglund, Doc. 1561 pp. 41–42, 114.)
Dr. Andrew Appel	Dr. Appel is the Eugene Professor of Computer Science at Princeton University and served as Chair of the Computer Science Department from 2009–15. Computer security is one of his primary areas of specialization. (Declaration of Andrew Appel, Doc. 1678-2 ¶¶ 1-6.)
Harri Hursti	Mr. Hursti is an internationally recognized security engineer, programmer, and “ethical hacker” who specializes in computer election security issues. (Declaration of Harri Hursti, Doc. 680-1 at ECF 37–43, ¶¶ 3–6.)
Defendants’ Experts in Prior Stages of this Case⁶	
Dr. Juan Gilbert	Professor Gilbert is a Professor and Chair of the Computer & Information Science & Engineering Department of the University of Florida. He served as one of the State Defendants’ experts previously in this case. His work focuses on individuals with disabilities’ access to technology, including voting technologies. (10/11/20 PI Order, Doc. 964 at 69.)
Dr. Michael Shamos	Dr. Shamos is a Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University and Director of the M.S. in

⁶ Defendants have given no indication at this juncture that these experts will be used in the current phase of this case or at trial. Rather, Plaintiffs cite to the testimony of Dr. Gilbert and Dr. Shamos in support of their arguments in opposition to Defendants’ summary judgment motions.

	Artificial Intelligence and Innovation at the Language Technologies Institute. He has participated in the examinations of electronic voting systems in a number of states and testified before an array of legislative bodies. He served as an expert witness for the Secretary of State in the 2019 preliminary injunction hearing dealing with the DRE voting machines. (July 10, 2019 Decl. of Michael Shamos, Doc. 472-1 ¶ 4.) He has not provided expert testimony in this case since 2019.
Data System Breach in Coffee County	
Cathy Latham	At the time of the events in Coffee County, Ms. Latham served as the Coffee County Republican Party Chair. (Aug. 8, 2022 Dep. of Cathleen Latham, Doc. 1471-1 p. 17.)
Misty Hampton	Ms. Hampton is the former Coffee County Elections Supervisor. (Nov. 11, 2022 Dep. of Emily Misty Hampton, Doc. 1610 p. 16.)
Scott Hall	Mr. Hall is a bail bondsman who informed Marilyn Marks during a phone call about the unauthorized access in Coffee County. He also acted as a leader in the Coffee County breach by directing SullivanStrickler's work on January 7, 2021. (Sept. 2, 2022 SullivanStrickler Rule 30(b)(6) Dep. of Dean Felicetti, Doc. 1489-2 p. 118; Transcript of Hall-Marks Call, Doc. 1364-1.)
Doug Logan	Mr. Logan is the CEO of a company called Cyber Ninjas. His business card was found on Misty Hampton's desk and he subsequently admitted to uploading Coffee County files to SullivanStrickler's ShareFile site. (Nov. 18, 2022 Dep. of Doug Logan, Doc. 1612 pp. 9, 125.)
Jeffrey Lenberg	Mr. Lenberg is a consultant who analyzed Dominion election management system software in person in both Coffee County, Georgia and Michigan. (Nov. 21, 2022 Dep. of Jeffrey E. Lenberg, Doc. 1613 p. 16.)
SullivanStrickler	SullivanStrickler is an Atlanta-based firm that was engaged by Jim Penrose and Doug Logan in January 2021 to forensically image data from the election equipment in the Coffee County Election Office. (Sept. 2, 2022 SullivanStrickler 30(b)(6)

	Dep. of Dean M. Felicetti, Doc. 1489-2 pp. 18–19, 28–29, 86.) Sidney Powell paid for the firm’s services. (<i>Id.</i> p. 75.) After collecting the data, SullivanStrickler employees uploaded that information to a ShareFile site, where it was further accessed by others. Additional copies were sent vis FedEx to attorney Stefanie Lambert in Michigan. (<i>Id.</i> pp. 174–78.)
Paul Maggio	Mr. Maggio is an employee of SullivanStrickler who uploaded all of the data acquired in Coffee County onto the Coffee County ShareFile. (Dec. 5, 2022 Decl. of Kevin Skoglund, Doc. 1635-44 ¶¶ 56–57.)
Dean Felicetti	Mr. Felicetti is SullivanStrickler’s Director of Data Risk & Remediation and Rule 30(b)(6) representative. (Sept. 2, 2022 SullivanStrickler Rule 30(b)(6) Dep. of Dean Felicetti, Doc. 1489-2 p. 14.)
Eric Chaney	Mr. Chaney is a former Coffee County Elections Board member. (August 15, 2022 30(b)(6) Dep. of Eric B. Chaney, Doc. 1471-11 pp. 13–14.)
Alex Cruce	Mr. Cruce is the data analyst who flew to Coffee County with Scott Hall. (Nov. 22, 2022 Dep. of Alex Andrew Cruce, Doc. 1614 pp. 71–73, 142.)
James Penrose	Mr. Penrose is the co-organizer of SullivanStrickler’s work in Coffee County and of Doug Logan and Jeffrey Lenberg’s later visits to the Coffee County Elections office. (Skoglund Decl., Doc. 1635-44 ¶¶ 17, 116.)
Charles Bundren	Mr. Bundren is an attorney and the co-organizer of SullivanStrickler’s work in Coffee County and of Doug Logan and Jeffrey Lenberg’s later visits to the Coffee County Elections office. (<i>Id.</i> ¶¶ 16, 71, 116, 142.)
Stefanie Lambert	Ms. Lambert is an attorney in Michigan who was mailed copies of materials that SullivanStrickler copied in Coffee County. She subsequently hired Benjamin Cotton to analyze the data. (<i>Id.</i> ¶¶ 77–78, 85.)
Michael Lynch	Mr. Lynch is a private investigator in Michigan who worked with Ms. Lambert. (<i>Id.</i> ¶¶ 79.)

James Barnes	Mr. Barnes replaced Misty Hampton as Coffee County Elections Supervisor after her February 2021 termination. (July 20, 2022 Dep. of James A. Barnes, Jr., Doc. 1630-17 p. 85.)
--------------	--

In addition to describing the individuals and entities relevant to this matter, the Court also provides a “Glossary of Terms” to clarify the meaning of various frequently used terms that appear in this Opinion and Order.

GLOSSARY OF TERMS

BMD Software

ImageCast X (“ICX”) Prime Ballot Marking Device (“BMD”)	An ImageCast X (“ICX”) Prime Ballot Marking Device (“BMD”) is an Android-based touch-screen device that allows voters to mark ballots on-screen and print them to an attached laser printer. (Redacted Expert Report of Dr. J. Alex Halderman “Redacted Halderman Report,” Doc. 1681 at 9.)
ICX App	An ICX App is an Android application developed by Dominion that is responsible for most of the BMD’s functionality. (<i>Id.</i> at 10.) The app is installed through a process called “side-loading” in which an Android application package (“APK”) file containing the software is uploaded from a USB device before each election in the form of an election definition file. (<i>Id.</i>) If an attacker were to obtain a copy of the APK file, he could potentially generate a new copycat APX file containing malicious code that could be installed in place of the real software. (<i>Id.</i> at 32.)
ImageCast Precinct (“ICP”) count scanner	An ImageCast Precinct (“ICP”) count scanner is a scanner used to count ballots produced by the BMD machines and those that are marked by hand in every county. (<i>Id.</i> at 11.)

Election Management System (“EMS”)	An EMS or election management system is “a collection of servers and computers that operate the Dominion Democracy Suite EMS application software.” (<i>Id.</i> at 49.) In Georgia, each county operates a separate election management system. (<i>Id.</i>)
QR Code	A QR code is a two-dimensional barcode that is intended to represent voters’ selections in machine-readable but not human-readable form. (<i>Id.</i> at 13.)
Smart Card	A smart card is a card that a BMD uses to authenticate technicians, poll workers, and voters. (<i>Id.</i> at 26–31.)
ImageCast Central (“ICC”) central-count scanner	An ImageCast Central (“ICC”) central-count scanner is a device used to record vote selections from hand-marked absentee ballots.
Pollbook	A pollbook is a database containing voter identification information by precinct. (8/15/19 PI Order, Doc. 579 at 25 n.22.)
PollPad	A PollPad is a device containing electronic Pollbook information. The PollPads are used to check in voters at the polls and generate voter access cards for the BMDs. (9/28/20 Paper Backup PI Order, Doc. 918 at 19 & n.8.)
Auditing	
Risk Limiting Audit (“RLA”)	<p>An RLA is defined by Georgia statute as “an audit protocol that makes use of statistical methods and is designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome.” O.C.G.A. § 21-2-498(a)(3). However, more precise and particularized descriptions and definitions of RLA methodology and results are discussed and explained in source academic literature, including that of Professor Stark.</p> <p>A 2022 report of the National Conference of State Legislature described these audits in this manner:</p>

	<p>“In recent years, researchers have developed statistically based audit techniques, referred to as risk-limiting audits (RLAs). These cut down on the number of ballots that need to be audited, while also providing statistical confidence that an incorrect election result is not certified (i.e., made official). As the name suggests, an RLA is designed to limit the risk that a contest is certified with the wrong winner. It does this by increasing the initial sample when discrepancies are found until either the level of confidence has been met or a full recount has been performed. RLAs are an incremental audit system: If the margin of an election is wide, very few ballots must be reviewed. If the margin is narrow, more will be reviewed up to the point that enough evidence is provided to confirm the declared election result.” (<i>Id.</i>)</p> <p>And the NCSL also notes that “A postelection audit may be able to detect whether any outside interference occurred, and security experts recommend them as one method of protecting the integrity of elections.”⁷ (<i>Id.</i>)</p> <p>Additionally, the NCSL Report found that, “All methods of RLAs require a voting system that produces a voter-verified paper audit trail” and modifications based on the type of voting equipment used. (<i>Id.</i>)</p>
Logic and Accuracy Testing	<p>Logic and accuracy testing is the process through which election officials verify in advance of an election that all voting equipment is properly functioning, including the BMD touchscreens, printers, scanners, and PollPads. (10/11/20 PI Order, Doc. 964 at 51.) Georgia’s particular mode of conducting logic and accuracy testing is abbreviated in its scope. (<i>Id.</i> at 51–60.)</p>

⁷ NCSL 2022 Report on Risk-Limiting Audits, <https://www.ncsl.org/elections-and-campaigns/risk-limiting-audits> (last visited October 11, 2023).

IV. Relevant Background

This election security case has been a long roller coaster ride, with many twists and turns. Below, the Court provides the background and context necessary to understand the current dispute and the legal issues before the Court. In so providing, the Court does not make any factual findings. And, as required at summary judgment, the Court presents the facts in the light most favorable to the non-moving parties — here, the Plaintiffs.

With that framing in mind, the Court first, in Section A, discusses the vulnerabilities and issues raised regarding the prior DRE voting system that existed at the onset of this case. While this system is no longer in operation, many of the very same concerns persist under the current BMD system. After addressing the litigation and prior findings about the old DRE system, the Court, in Section B, charts the State's transition from the DRE system to the current BMD system. Next, in Section C, the Court outlines Plaintiffs' challenges to the constitutionality of the current BMD system. Then, in Section D, the Court reviews the concerns presented by the Plaintiffs at the 2020 preliminary injunction hearing, including their central concerns related to the QR barcodes used to tabulate votes and the auditability of the BMD system more broadly (among other issues). After that, in Section E, the Court traces newer post-2020 developments regarding these same vulnerability concerns. These new developments include: the issuance of a comprehensive report by Plaintiff's expert, Dr. Alex Halderman, regarding the

vulnerabilities of the BMD system; the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Agency’s (“CISA”) review and corroboration of Dr. Halderman’s central findings; the results of a 2021 technical assessment conducted by the State’s retained consulting cybersecurity firm, Fortalice; and, of course, the now infamous breach of the election system in Coffee County, Georgia and the State’s response to this breach. Finally, the Court addresses the present posture of the case in Section F.

In outlining the landscape of this case, the Court has endeavored to be thorough, and, as such, asks the reader to buckle up and bear with the ride.

A. The Vulnerabilities of the Previous DRE System (And Why They Are Still Relevant)

Plaintiffs filed this lawsuit in 2017, raising constitutional challenges to the election system that was then in place in Georgia. (Original Complaint, Doc. 1-2.)⁸ This integrated system (“the DRE system”) was composed of the Direct Recording Electronic voting machines (“DREs”), the Global Election Management Systems (“GEMS”) servers, and the online voter registration database. (*See generally id.*) In the original complaint, Plaintiffs alleged that the system was compromised, had not been properly examined and tested prior to the election as required by state law, and was vulnerable to outside manipulation. Plaintiffs’ original complaint thus alleged that the State’s continued use of the DRE system unconstitutionally burdened their fundamental right to vote and denied them equal protection of the

⁸ The case was initially filed in the Superior Court of Fulton County on July 3, 2017. Defendants removed the case to this Court shortly thereafter.

laws as compared to voters using paper ballots, all in violation of the First and Fourteenth Amendments. (*See id.* ¶¶ 120–52.)

1. The Court’s 2018 Preliminary Injunction Order Finds Serious Vulnerabilities in the DRE System

In the summer of 2018, Plaintiffs filed motions for preliminary injunction in which they sought, among other things, to enjoin the State from using the DRE system in the November 2018 general election.⁹ (*See* Motions for PIs, Docs. 258, 260, 271.) In support, Plaintiffs presented evidence demonstrating that the State’s central election server — maintained by Kennesaw State University’s (“KSU”) Center for Election Services (“CES”) on behalf of the Secretary of State’s Office — was publicly accessible on the internet from at least August 2016 to March 2017. (9/17/2018 PI Order, Doc. 309 at 7–8.) In particular, Plaintiffs presented evidence that, in August 2016, a professional cybersecurity expert, Logan Lamb, discovered that he could access, via CES’s public website, multiple gigabytes of election data, as well as thousands of files with private elector information (including home addresses, birth dates, and more). (*Id.*) In addition, Lamb was able to access (again, via the internet) the election management databases for at least 15 counties — databases used to create ballot definitions; program memory cards; and tally, store, and report all votes — as well as passwords that polling place supervisors used to administer corrections to the DRE machines. (*Id.*) Lamb immediately

⁹ By that point the Plaintiffs had broken into two separate groups — the Curling Plaintiffs and the Coalition Plaintiffs — and were represented by separate counsel.

alerted the Executive Director overseeing CES, Merle King, of his discovery. Despite this notification, no remedial action was taken at that time. (*Id.*)

Months later, in February 2017, one of Lamb’s cybersecurity colleagues (Chris Grayson) discovered that he was able to repeat what Lamb had done and thus access the same key election data. (*Id.*) On March 1, Grayson notified another colleague at KSU and, ultimately, through a chain of events, Executive Director of CES King was notified again. (*Id.* at 8–9.) Days later, the FBI was alerted and took temporary possession of the CES server.

A few months after that, on July 7, 2017 — four days after this lawsuit was originally filed in Fulton County Superior Court — all data on the hard drives of KSU’s “elections.kennesaw.edu” server was destroyed by KSU/CES.¹⁰ The next month, on August 9, 2017 — a day after this action was removed to this Court — all data on the hard drive of a secondary server, which contained similar information to the “elections.kennesaw.edu” server, was also destroyed by KSU/CES. (*Id.* at 9.)

After these events, the Secretary of State’s Office shut down the CES and absorbed its functions as of January 1, 2018. (*Id.* at 7, 9; *see also* 8/15/19 PI Order, Doc. 579 at 63.) The only CES staff member transferred to the State was Michael Barnes, a KSU/CES Director who reported to Executive Director King. (9/17/2018 PI Order, Doc. 309 at 35.) Mr. Barnes had a degree in public administration but no

¹⁰ In the Court’s 2020 PI Order, it made clear that it was KSU that destroyed the servers. (10/11/2020 PI Order, Doc. 964 at 14 n.9)

formal training or expertise in computer science or cybersecurity. (*Id.* at 35 n.26; *see also* 8/15/19 PI Order, Doc. 579 at 63 n.47.) After his January 2018 transfer to the Secretary of State’s Office, Mr. Barnes continued (and continues to this day) as a Director of CES to play a major role in management of the electronic election system.

After holding a hearing on the preliminary injunction motions, the Court ultimately (1) found that Plaintiffs had shown that the DRE system “pose[d] a concrete risk of alteration of ballot counts that would impact their own votes,” *but* (2) declined to grant injunctive relief because requiring Defendants to make a last-minute switch to a different election system would undermine the government’s and the public’s interest in the orderly administration of elections. (9/17/18 PI Order, Doc. 309 at 38, 41–44.) Although the Court did not grant injunctive relief, it “expressly warned Defendants that further delay by the State in remediating its technologically outdated and vulnerable voting system would be intolerable.” (8/15/19 PI Order, Doc. 579 at 3) (discussing 9/17/18 PI Order, Doc. 309 at 44.)

2. The Court’s 2019 Preliminary Injunction Order Finds “A Catalogue of Pervasive Problems” Concerning the DRE System and Enjoins the State From Using the DREs After the 2019 Election

In late spring of 2019, Plaintiffs filed another round of motions for preliminary injunction seeking to enjoin Defendants from using the DRE system in the November 2019 local/municipal elections. (*See* Docs. 387, 419.) As relief, Plaintiffs sought relief requiring Defendants to use hand-marked paper ballots

(“HMPBs”) for the 2019 elections instead of the DREs. (See 8/15/19 PI Order, Doc. 579 at 4.) Plaintiffs also sought to require Defendants to address ongoing issues with the voter registration database, which Plaintiffs contended was “riddled with data reliability and accuracy problems that result in the unconstitutional disenfranchisement and burdening of voters’ rights to cast regular ballots that are actually counted.” (*Id.*)

After a hearing, the Court granted in part and denied in part Plaintiffs’ 2019 preliminary injunction motions on August 15, 2019. (*Id.* at 152.) The Court found that Plaintiffs had presented evidence of “a catalogue of pervasive voting problems arising in the 2017-2018 election period” that had “compound[ed] and expand[ed] the evidence established in the September 2018 preliminary injunction record.” (*Id.* at 5.) This evidence demonstrated that Georgia’s election system burdened the Plaintiffs’ right to cast secure, reliable ballots that were accurately counted. (*Id.*) Those “pervasive voting problems” included, among other things, the lack of a ballot paper trail, outdated operating systems and software, and further developments regarding the breach of the election servers at KSU, as discussed below.

a. Problems With the Lack of a Paper Voting Trail

First, the Court recognized that, because the DREs did not include a paper voting trail, “No voters could verify whether their intended votes for particular candidates were actually cast.” (*Id.* at 92.) The lack of a paper voting trail was particularly concerning because of the risk of undetectable cyberattacks on the

DREs. As a seminal report on voting systems from the National Academies of Sciences (“NAS”) emphasized, “any voting system should allow a voter to verify that the recorded ballot reflects his or her intent, which isn’t possible with paperless DRE machines.” (*Id.* at 39) (quoting National Academies of Sciences, Engineering, and Medicine, et al., *Securing the Vote: Protecting American Democracy* 42, 80 (National Academies Press, 2018)). The NAS report recommended that “voting machines that do not produce paper audit trails ‘be removed from service as soon as possible.’” (*Id.* at 40) (quoting NAS report.) Likewise, a 2019 report from the Senate Select Committee on Intelligence (“SSCI report”) recommended that states discontinue using DREs on similar grounds, noting that the machines “are now out of date.” (*Id.* at 41) (quoting 2016 U.S. Election, Vol. 1: Russian Efforts Against Election Infrastructure with Additional Views, 116th Cong., 1st Session (2019).)

b. Problems With Outdated Operating Systems and Failure to Implement Security Patches

In the 2019 PI Order, the Court next noted that one component of the DRE system — the GEMS server — was running on an outdated Windows XP/2000 operating system, and the DRE machines were operating on software *from 2005* that was so out of date that the makers of the software were no longer supporting it or providing security patches.¹¹ (*Id.* at 22, 25.) The evidence further showed that,

¹¹ The evidence also revealed that outside contractors for the Secretary of State’s CES unit were using the GEMS server application on their *home computers* to build the ballots to be used on the

for years, the State had failed to implement critical software patches, including a software patch that was necessary to address a vulnerability that “ethical hacker” and cybersecurity specialist Harri Hursti discovered in 2006. The State Defendants’ own expert at that time, Dr. Michael Shamos, described this particular vulnerability as “one of the most severe security flaws ever discovered in a voting system,’ up to that time.” (*Id.* at 23) (quoting Deposition of Michael Shamos, Doc. 554.)

c. Slow and Ineffective Response to KSU Data Breach

Next, the Court reviewed newly available evidence regarding the CES/KSU data breach, data systems mismanagement, and record destruction events previously addressed in the 2018 PI Order. The expanded record revealed additional troubling details regarding the breach. In particular, the evidence demonstrated the extent of Mr. Lamb’s exhaustive efforts to bring security issues to CES Executive Director King’s attention — including issues related to: the public accessibility of the election server; grossly out-of-date essential windows software; the use of particular software that was subject to malware for which there was a public advisory; and anonymous users’ access to data files. (8/15/19 PI Order, Doc. 579 at 65.)

The expanded record also revealed the extent to which CES Director Michael Barnes was aware of Lamb’s August 2016 warning email regarding the above-

DREs. It was unclear what security protocols, if any, these contractors had been following. (*Id.* at 32.)

described vulnerabilities and the extent to which he was aware that KSU Information Office staff *had confirmed* these serious software threats, website holes, and data-security exposures *as of October 2016*. (*Id.* at 65–67.)

The supplemented record also showed the extensive efforts expended to inspire responsive action from CES. In fact, it was only after (1) Lamb’s cybersecurity colleague (Grayson) contacted another colleague at KSU (Andy Green) in February 2017; (2) Green — after himself confirming the server exposure — contacted KSU Chief Information Officer (Stephen Gay) in the University’s Information Security Office (independent of CES); and (3) Gay — after having his independent security team further confirm the system vulnerabilities — contacted CES’s Executive Director Merle King, that any responsive action was taken to close down the server and contact federal investigators. (*Id.* at 67–68.) Moreover, in confirming the system vulnerabilities, Gay’s Information Security Office’s team discovered, on March 4, 2017, that one of the exposed files contained 5.7 million records with personal identifying information. (*Id.* at 68.)

A detailed incident report issued on April 18, 2017 identified the seriousness and extensiveness of the issues posed by CES’s and KSU’s handling of its IT systems. (*Id.*) But there was no evidence that measures were taken to assess the integrity of the election data (such as, e.g., checking for malware) that was ultimately transferred from the CES/KSU server to the Secretary of State’s server. (*Id.* at 69.)

d. Problems With the Voter Registration Database

In addition, the Court found in its 2019 Order that Plaintiffs presented significant evidence of vulnerabilities in the State’s voter registration database in connection with the previously discussed exposure of voter data, the exposure of passwords, and outdated software issues.¹² The Court additionally noted that the voter registration database, in tandem with operational software, “play[s] a vital role in the proper functioning of the voting system.”¹³ (*Id.* at 88–90.)

e. Insufficient Remedial Action

Following the KSU breach, the Secretary of State’s Office absorbed the functions of the CES in January 2018. However, the State still insisted that despite the “gaping breach and exposure of the CES/KSU system and voter database” that “nothing amiss happened.” (*Id.* at 70.) The Court found that this position “contradict[ed] the evidence.” (*Id.*) And although all the data on the hard drives associated with the election server and a secondary server were mysteriously destroyed a mere four days after Plaintiffs filed this lawsuit, Defendants argued that the servers had simply been “repurposed” instead of wiped or destroyed. (*Id.* at 65.) The Court found that this was not credible. (*Id.* at 70.)

¹² The State’s retained cybersecurity firm, Fortalice, found that the Secretary of State’s then-contractor for maintenance of its voter registration database, PCC, continued to use outdated software which needed patches. (8/15/19 PI Order, Doc. 579 at 88.)

¹³ Because the voter registration database and electronic pollbooks could be accessed over the Internet, the SSCI report considered them to be “vulnerable components of U.S. election infrastructure.” (8/15/19 PI Order, Doc. 579 at 41–42.) Based on these vulnerabilities, the SSCI report recommended that states update the software for their voter registration databases and create paper backups of their pollbook information. (*Id.* at 42.)

Further, although the State had argued that they had taken some remedial action by retaining Fortalice Solutions Company (“Fortalice”), a highly-qualified forensic consulting firm, to perform three cybersecurity assessments for the Secretary of State’s office, the Court found that these assessments were decidedly limited in scope. As the Court noted, “[i]t was outside Fortalice’s contract scope to focus on particular Election Division or GEMS data systems or conduct a review of the voter registration system software and operation, or the state election data systems’ interface with SOS servers and SOS and County data systems and the cybersecurity and vulnerability issues posed by this interface.” (*Id.* at 77.) As a result, “the surface of SOS cybersecurity issues was barely scratched.” (*Id.* at 76.) Moreover, even with these limitations, Fortalice identified 22 cybersecurity risks in its first assessment in October 2017, with 10 identified as high priority for remediation action. (*Id.* at 77.) And it later identified an additional 15 risks in its second assessment in February 2018, including what the Court described as “an astonishingly grave array of deficits” in the software used to maintain the voter registration database and in the Secretary of State’s Office’s handling of the database. (*Id.* at 82.) In its third assessment in November 2018, Fortalice determined that the State had remedied just three of the 22 risks identified in the first assessment from a year earlier, in addition to making 20 additional cybersecurity recommendations, 14 of which were low to no cost. (*Id.* at 84.)

Based on all of this evidence, the Court stated, as it had in the 2018 PI Order, that “the State had ‘stood by for far too long’ in failing to address the ‘mounting

tide of evidence of the inadequacy and security risks’ posed” by the DRE system. (*Id.* at 3) (quoting 9/17/18 PI Order, Doc. 309 at 43). Even so, after considering all the evidence, the Court found that the balance of the equities, law, and the public interest weighed against granting Plaintiffs’ request for an Order requiring a HMPB system for the 2019 election cycle while it was in the process of transitioning to a new statewide voting system for future elections (at discussed next). But, the Court still directed the State Defendants to refrain from using GEMS/DRE election system after 2019. (*Id.* at 139, 148.) The Court also directed, among other remedial relief measures, the Secretary of State’s Office to work with its consulting cybersecurity firm (Fortalice) to conduct an in-depth review and formal assessment of issues relating to vulnerability and accuracy of the voter registration database, as discussed in the 2018 and 2019 Orders, as well as other election data system issues that would likely migrate with the State’s transition of voting system to the new voting system authorized by the legislature in 2019.

B. Georgia’s Transition From the DRE to the New Dominion BMD System in 2019

In the midst of this litigation, the State enacted legislation requiring a switch to a new election system — the Ballot-Marking Device (“BMD”) system.

1. The Georgia Legislature Passes HB 316

In April 2019, the Georgia State Legislature enacted House Bill No. 316 (“HB 316”) — a new law requiring the Secretary of State to replace the DRE system with electronic ballot-marking devices and optical scanners. (*See* 8/7/20 PI Order, Doc.

768 at 3.)¹⁴ HB 316 requires the State to switch to a new voting system that uses “electronic ballot markers” for all in-person voting in federal, state, and county elections.¹⁵ O.C.G.A. § 21-2-300(a)(2). The statute requires that electronic ballot markers “produce paper ballots which are marked with the elector’s choices in a format readable by the elector” and that votes are counted by scanners. *Id.* The legislation further stipulated that the associated election equipment must be certified by the U.S. Election Assistance Commission, and that the State switch to the new system “[a]s soon as possible, once such equipment is certified by the Secretary of State as safe and practicable for use.” *Id.* § 21-2-300(a)(2), (a)(3).

HB 316 also included new requirements regarding audits. In particular, the provisions require election superintendents to perform pre-certification audits “in accordance with requirements set forth by rule or regulation of the State Election Board.”¹⁶ *Id.* § 21-2-498(b). Accordingly, the State Election Board (“SEB”) later issued a rule requiring every county to participate in one audit of a single statewide race, selected by the Secretary of State, after the November general election in even

¹⁴ While HB 316 was signed into law on April 2, 2019, the contract, bidding, award, and implementation processes took time and the Secretary of State did not issue an order decertifying the DRE system until December 30, 2019, which was several months after the Court resolved the 2019 PI Motions in August 2019. (State Defs.’ Statement of Undisputed Material Facts “State Defs.’ SUMF,” Doc. 1569 ¶ 3, 29.)

¹⁵ The statute defines an “[e]lectronic ballot marker” as “an electronic device that does not compute or retain votes; may integrate components such as a ballot scanner, printer, touch screen monitor, audio output, and navigational keypad; and uses electronic technology to independently and privately mark a paper ballot at the direction of an elector, interpret ballot selections, communicate such interpretation for elector verification, and print an elector verifiable paper ballot.” O.C.G.A. § 21-2-2(7.1).

¹⁶ The State Election Board is responsible for issuing rules and regulations pertaining to election audit procedures, including “security procedures to ensure that collection of validly cast ballots is complete, accurate, and trustworthy throughout the audit.” *Id.* § 21-2-498(d).

numbered years — i.e., one audit of a single statewide race every two years. *See* Ga. Comp. R. & Regs. 183-1-15-.04(1). By statute, these audits must be performed “by manual inspection of random samples of the paper official ballots.” O.C.G.A. § 21-2-498(b).

Additionally, *at the time it was enacted*, the statute contained an additional provision requiring the Secretary of State to select at least one county to perform a risk-limiting audit pilot program by December 31, 2021.¹⁷ *See* O.C.G.A. § 21-2-498 (2019). This provision also required the Secretary of State to review the pilot program and provide the General Assembly with a “comprehensive report, including a plan on how to implement risk-limiting audits state wide.” *Id.* Finally, if this risk-limiting audit pilot program was successful in achieving the specified confidence level, the provision required that “all audits performed pursuant to this Code section shall be similarly conducted, beginning not later than November 1, 2024.” *Id.* However, this provision was later removed from the statute and other provisions were also weakened in 2023. (*See* Ex. 1, Pls.’ Notice of Change of State Law on Audits, Doc. 1673.)

2. The Secretary of State Issues Notice of Intent to Award Contract to Dominion

On July 29, 2019, the Secretary of State issued a Notice of Intent to award a contract for the State’s new voting system to Dominion Voting Systems, Inc.

¹⁷ The relevant section of the election code defines a “[r]isk-limiting audit” as “an audit protocol that makes use of statistical methods and is designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome.” *Id.* § 21-2-498(a)(3).

(“Dominion”). (Decl. of Ryan Germany, Doc. 1569-3 ¶¶ 3–4.) The contract required the new voting system to be fully implemented by March 24, 2020. (*Id.*) The State ordered 30,050 BMDs under the contract and began working to implement the new system. (*Id.* ¶ 5; State Defs.’ Statement of Undisputed Material Facts (“State Defs.’ SUMF”) Doc. 1569 ¶ 9.)

3. How the BMD System Functions

The voting system the State ultimately selected — Dominion Democracy Suite — includes the following components: BMDs and associated printers, ICC scanners (used to count hand-marked absentee ballots) and ICP scanners (used to count ballots produced by the BMD machines), Dominion’s EMS software, and electronic PollPads. (Decl. of Dr. Eric D. Coomer “Coomer Decl.,” Doc. 1569-4 ¶ 3; Pls.’ Corrected Joint Statement of Additional Facts, Doc. 1637 ¶ 79.) While the State purchased entirely new equipment from Dominion, it continued to use existing voter data from the ENET system to operate the PollPads. (Feb. 2, 2022 30(b)(6) Dep. of Sanford Merritt Beaver, Doc. 1628-31 pp. 19–21; *see also* 10/11/20 PI Order, Doc. 964 at 16.)

In a prior Order, the Court described the process of voting on Dominion’s BMD system as follows:

Pollworkers use the ePollbook to confirm a voter is in the correct polling place and eligible to vote and then to encode and issue a voter access card. The voter inserts the access card into the BMD which pulls up the ballot style assigned to the voter encoded on the access card and displays voting options on the BMD touchscreen. After the voter makes her selections on the touchscreen, the BMD prints a paper ‘ballot’ containing a 2D barcode encoded with the selections and a human readable text summary of the voter’s selection The voter

is expected to review the human readable summary on the paper ballot printout to confirm that it correctly reflects the choices made on the touchscreen before casting her ballot by inserting it into a separate ballot scanner. The summary indicates the candidates for whom a vote was cast, but not the other candidates identified in each race.

(7/30/20 MTD Order, Doc. 751 at 4–5) (internal citations omitted).

Notably, in the particular variation of the Dominion BMD system chosen by the State, the scanners count in-person votes based on the selections *contained within the QR codes* on the printouts — *not the selections that appear on the human-readable text*. (Pls.’ Corrected Joint Statement of Additional Facts, Doc. 1637 ¶ 87; see Coomer Decl., Doc. 1569-4 ¶ 9 (“Dominion’s optical scanners (ICP) can be used with BMD-marked paper ballots or hand-marked paper ballots. The ICP units do not interpret the human-readable (text) portion of either type of ballot. Instead, the ICP units are programmed to read the QR Code for the BMD ballot or particular coordinates on hand marked ballot.”)). The QR codes are *not encrypted*. (Redacted Halderman Report, Doc. 1681 at 20.) Once the scanner records the information from the QR code, the scanner then saves this information — i.e., the cast vote record — to removable flash cards for use by county election officials for final tabulation. (7/30/20 MTD Order, Doc. 751 at 6.)

While the scanners count the in-person votes based on the QR codes, in the event of a recount (conducted pursuant to O.C.G.A. § 21-2-495) or an audit (conducted pursuant to O.C.G.A. § 21-2-498), the human-readable text governs instead of the QR code tabulation. O.C.G.A. § 21-2-379.23(d). Although another version of Dominion’s BMD system allows the scanners to tabulate votes based on

the human-readable text without the QR codes, that system has not yet been adopted in Georgia. (Pls.’ Corrected Joint Statement of Additional Facts, Doc. 1637 ¶ 86.)

The BMD system was used for the first time on a statewide basis in Georgia in the June 9, 2020 presidential primary election.¹⁸ (See 8/17/20 PI Order, Doc. 768 at 9–10.) Currently, the BMD system is being used for elections in all Georgia counties. (State Defs.’ SUMF, Doc. 1569 ¶ 10.)¹⁹

C. Plaintiffs’ Amended Complaints and Challenges to the Constitutionality of the New BMD System and the State’s Motion to Dismiss

On October 15, 2019, both sets of Plaintiffs amended their Complaints to assert constitutional challenges to the BMD system. (See Curling Pls.’ Third Am. Compl., Doc. 627; Coalition Pls.’ First Suppl. Compl., Doc. 628.)²⁰ Specifically, the Curling Plaintiffs raised three substantive claims challenging the BMD system: a violation of the fundamental right to vote under the Due Process Clause of the Fourteenth Amendment (Count III), an Equal Protection Clause claim alleging that in-person voters using the BMD system are deprived of equal protection as

¹⁸ The original March 24, 2020 rollout date was pushed back as a consequence of the COVID-19 pandemic. (8/17/20 PI Order, Doc. 768 at 9–10.)

¹⁹ As of November 2020, approximately twenty-four states used one or more components of the Dominion Democracy Suite voting system. (Redacted Halderman Report, Doc. 1681 at 9.) Most of these jurisdictions provided BMDs *solely* to voters upon request for disability voting accessibility purposes or in specific counties. Georgia and South Carolina were the only states to use BMDs as the primary method of voting statewide. (*Id.*)

²⁰ The Curling Plaintiffs’ Third Amended Complaint challenges both the DRE system and the BMD system. The Coalition Plaintiffs’ First Supplemental Complaint only challenges the BMD system; however, the Coalition Plaintiffs continue to maintain their challenges to the DRE system that they previously included in their Third Amended Complaint. (See Coalition Pls.’ Third Am. Compl., Doc. 226.)

compared to voters using absentee paper ballots (Count IV), and a request for a declaratory judgment that the QR code system fails to comply with HB 316's statutory requirement for an elector-verifiable paper ballot. (Curling Pls.' Third Am. Compl., Doc. 627 ¶¶ 113–40.)

The Coalition Plaintiffs similarly alleged that the BMD system violated their fundamental right to vote under the First and Fourteenth Amendments (Count I) and the Equal Protection Clause (Count II), and also raised a procedural due process claim (Count III). (Coalition Pls.' First Suppl. Compl., Doc. 628 ¶¶ 221–45.) The Coalition Plaintiffs similarly request relief as to the QR codes. In addition to raising these three claims, the Coalition Plaintiffs also included — as a component of Counts I and II — an argument that the BMD system both infringed upon their fundamental voting rights by denying them the right to cast a secret ballot in person and denied them equal protection of the laws compared to absentee voters who were permitted to cast a secret ballot. (*See, e.g., id.* ¶ 223.)

In short order, the State Defendants moved to dismiss Plaintiffs' Amended Complaints, (Doc. 645), which the Court ultimately granted in part and denied in part (7/30/20 MTD Order, Doc. 751 at 52). In its Order, the Court dismissed the Curling Plaintiffs' declaratory judgment claim and the Coalition Plaintiffs' procedural due process claim without prejudice, but permitted Plaintiffs'

remaining claims to proceed. (*Id.*)²¹ Thus, as to the BMD claims, the Curling Plaintiffs’ Counts III and IV remain, as do the Coalition Plaintiffs’ Counts I and II.

D. The Court’s 2020 Preliminary Injunction Order Addresses Vulnerabilities of the BMD System

In August 2020, Plaintiffs filed their next round of motions for preliminary injunction, now raising challenges to Defendants’ implementation of the BMD system. (*See* Docs. 785, 809.) In their motions, Plaintiffs argued that the BMD system suffered from many of the same deficiencies as the DRE system. According to Plaintiffs, because the BMD system was not secure, reliable, or voter verifiable, it unconstitutionally burdened their right to cast effective votes that would be accurately counted. In particular, the Plaintiffs raised concerns regarding *inter alia* the QR codes vulnerability to alteration or manipulation, questions about the auditability of the new BMD system, and the State’s significant failure to implement necessary elections software upgrades. The Coalition Plaintiffs also separately raised issues related to ballot secrecy, the optical scanner settings used to read absentee ballots, and problems with the voter information provided to the counties on the pollbooks and PollPads.

²¹ The Curling Plaintiffs did not oppose dismissal of their declaratory relief claim (Count V). (*See* 7/30/20 Order, Doc. 751 at 30 n.18.) The Court dismissed the Coalition’s procedural due process claim (Count III) because the Coalition Plaintiffs did not allege “that the State Defendants have failed to provide adequate procedures to remedy the alleged harms,” especially where they could seek relief in the state courts via a writ of mandamus. (7/30/20 Order, Doc. 751 at 49–51.) The Court notes that, in a recent decision, the Georgia Court of Appeals found that the BMD’s QR code system in fact does comply with HB 316’s voter-verifiable paper ballot requirement, though this decision has been appealed. *See VoterGA et al. v. State*, 889 S.E.2d 322 (Ga. Ct. App. 2023), *appeal filed*, S23C1132 (Ga. July 13, 2023).

As relief, both sets of Plaintiffs sought to require Defendants to utilize HMPBs (hand-marked paper ballots) and conduct a larger number and more meaningful audits of various types (pre-certification, post-election, and manual tabulation audits) for the 2020 election. (*See* 10/11/20 PI Order, Doc. 964 at 2.) The Court held lengthy hearings on September 8–9, 2020 on Plaintiffs’ preliminary injunction motions.

1. Concerns Regarding QR Code Vulnerability to Alteration

As discussed above, the BMDs generate paper printouts that include both a list of the voter’s selections and a QR code intended to reflect those selections. The printout is then fed into a separate ballot scanner that records the information *from the QR code, not the list of the voter’s selections*. The scanner saves the QR code information to removable flash cards that are used for tabulating results. (7/30/20 MTD Order, Doc. 751 at 6.) Plaintiffs argued that this system is problematic because: (1) the machines that generated the printouts were vulnerable to hacking/manipulation that could result in the alteration of either the human-readable text or the selections contained in the QR codes; (2), Plaintiffs could not verify whether the QR codes accurately reflected their selections; and (3) the printouts could not be meaningfully audited. (*See* 10/11/20 PI Order, Doc. 964 at 19–20.)

In support of their motion, the Curling Plaintiffs relied on evidence from their cybersecurity expert, Dr. Alex Halderman. At the hearing, Dr. Halderman demonstrated how malicious actors could potentially infiltrate the voting system

through various cyberattacks, including attacks that would cause particular votes to be changed or deleted, or enable the alteration or manipulation of the unencrypted QR codes.²² (*Id.* at 24–25.) In its 2020 PI Order, the Court noted that Dr. Halderman’s findings were consistent with a “broad consensus” among the nation’s cybersecurity experts that electronic voting systems, such as the BMD system, are susceptible to malware. (*Id.* at 26.) The same experts also agreed that these vulnerabilities “take on greater significance” in the context of a BMD system, like Georgia’s, because it relies on unauditable QR codes for counting votes that cannot be read and verified by the voters before tabulation. (*Id.*).

2. Concerns Regarding Lack of Auditing Ability and Frequency of Audits

The Plaintiffs also raised issues concerning the State’s ability to audit the functionality of the BMDs, specifically in the event that the selections contained within the QR codes did not match the selections that appear in the human-readable text (for example, if the QR codes had been altered). (*Id.* a 67–68.) At the hearing, the State Defendants argued that audits would look to the human-readable text – not the QR codes. (*Id.* at 71–72.) Plaintiffs argued that audits would not necessarily remediate this issue because most voters do not review each of their selections contained in the human-readable text. This would not allow the

²² Days before the hearing, Dr. Halderman was for the first time provided access to a BMD and the software variation that was used on the Georgia BMDs. He also used optical scanners/tabulators programmed with Dominion’s software. (10/11/20 PI Order, Doc. 964 at 24.) Dr. Halderman explained that he would need additional time to test the equipment given the compressed timeframe.

printouts to be properly audited against the QR data – and the review in this case was made particularly more difficult by the tiny print on the printout ballot that did not look like the ballot shown on the BMD. (*Id.* at 20.) In support, Plaintiff presented, among other things, evidence from a study conducted by Dr. Halderman and other researchers from the University of Michigan, in which only 6.5% of voters noticed when the printouts from BMD machines included human-readable text that had been altered so that it did not contain the selections that the voters had actually chosen. (*Id.* at 68.)

Plaintiffs also took issue with the infrequency of audits. In particular, they argued that auditing a single statewide race every two years was insufficient to verify that their votes were being correctly counted because the results of these audits would not address any down-ballot contests or contests that occurred in other election cycles.²³ These issues, among others, were addressed at length by the Coalition Plaintiffs’ expert, Dr. Philip Stark. (*See, e.g., id.* at 72–73.)

3. Concerns Regarding Software Upgrades

Plaintiffs also presented evidence that a Dominion software upgrade was available that would enable the scanners to capture voters’ selections as reflected in the human-readable text of the printouts from the BMDs (i.e., “full face ballots”) — which voters could read and verify — instead of the QR codes. (*See, e.g., id.* at 17

²³ As a reminder, HB 316 requires election superintendents to perform pre-certification audits “in accordance with requirements set forth by rule or regulation of the State Election Board.”²³ *Id.* § 21-2-498(b). The SEB has issued a rule requiring every county to participate in one audit of a single statewide race selected by the Secretary of State after the November general election in even numbered years. *See* Ga. Comp. R. & Regs. 183-1-15-.04(1).

n.19.) In its Order, the Court remarked that it could not fathom why the State would not at least be moving toward consideration of that option. (*Id.* at 146–47.)

4. The Court’s Rulings on the 2020 PI Order

After the hearing, the Court found that the evidence before it revealed “serious system security vulnerability and operational issues” that adversely affected Plaintiffs’ right to cast an effective vote that is accurately counted. (*Id.* at 143.) The Court explained that “[t]he substantial risks and long-run threats posed by Georgia’s BMD system, at least as currently configured and implemented, are evident.” (*Id.* at 89.) Nevertheless, the Court explained that “[w]hile [it] recognizes Plaintiffs’ strong voting interest and evidentiary presentation that indicate they may ultimately prevail in their claims,” the State’s administrative interests associated with managing a fast-approaching election and the challenges involved in a sweeping change in balloting methods weighed against granting broad injunctive relief. (*Id.* at 84.) The therefore Court concluded,

Ultimately, the Court must find that imposition of such a sweeping change in the State’s primary legally adopted method for conducting elections at this moment in the electoral cycle would fly in the face of binding appellate authority and the State’s strong interest in ensuring an orderly and manageable administration of the current election, consistent with state law. So, for this reason alone, despite the strength of Plaintiffs’ evidence, the Court must decline the Plaintiffs’ Motions for Preliminary Injunction.

(*Id.* at 89.)²⁴

²⁴ At that time, the Court also ruled on the Coalition Plaintiffs’ separate challenges relating to ballot secrecy, scanner settings for absentee ballot tabulation, and paper backups of the pollbooks provided by the State to counties. The Court addresses these three component parts of the Coalition Plaintiffs’ relief requests — which are separate and distinct from the broader challenge to the BMD system — at greater length in Section V.D. of this Order, and so does not do so here.

E. Post 2020 Developments and Plaintiffs' Additional Cited Evidence of Vulnerabilities of the BMD System

The parties built a considerable evidentiary record in the years leading up to the Court's 2020 preliminary injunction orders. That record has substantially grown in the nearly three years since. The most significant new evidence related to Plaintiffs' assertions of BMD system vulnerability includes: Dr. Halderman's 2021 Report, the CISA Report, Fortalice's 2021 Technical Assessment, and the 2021 voting system breach in Coffee County.

1. Dr. Halderman's July 2021 Report Identifies 7 Core Vulnerabilities

On July 1, 2021, Dr. Halderman, submitted a detailed, lengthy Report both (1) expounding on his prior testimony in this case and (2) identifying additional vulnerabilities he found in the BMD system, based on his testing of a BMD and associated election equipment provided to him by Fulton County. (*See Redacted Halderman Report, Doc. 1681.*)²⁵ To test the BMD and other election equipment, Dr. Halderman and his assistant spent multiple weeks studying the voting equipment, testing the equipment for vulnerabilities, and developing proof-of-concept attacks, which Dr. Halderman contended could purportedly be effectuated by malicious actors. (*Id.* at 4.)

²⁵ Besides testing the BMD, Dr. Halderman, over a specific and authorized time period, examined and had access to other equipment including the ICP scanner, a Poll Worker Card, a Technician Card, a USB drive containing an ICX election definition file, and an off-the-shelf HP LaserJet printer used to print ballots. (*Id.* at 18.) Dr. Halderman was *not* provided access to the Democracy Suite EMS software — software that was later compromised in the Coffee County breach.

In the Principal Findings section of his Report, Dr. Halderman determined that the BMD and related voting equipment suffered from “critical vulnerabilities” that could “be exploited to subvert all of [the BMD’s] security mechanisms.” (*Id.* at 4–5.) In particular, Dr. Halderman identifies seven primary vulnerabilities, as follows:

1. Attackers can alter the QR codes on printed ballots to modify voters’ selections (*id.* at 4–5);
2. Anyone with brief physical access to the BMD machines can install malware onto the machines (*id.* at 5);
3. Attackers can forge or manipulate the smart cards that a BMD uses to authenticate technicians, poll workers, and voters, which could then be used by anyone with physical access to the machines to install malware onto the BMDs (*id.*);
4. Attackers can execute arbitrary code with supervisory privileges and then exploit it to spread malware to all BMDs across a county or state (*id.*);
5. Attackers can alter the BMD’s audit logs (*id.*);
6. Attackers with brief access to a single BMD or a single Poll Worker Card and PIN can obtain the county-wide cryptographic keys, which are used for authentication and to protect election results on scanner memory cards (*id.*); and
7. A dishonest election worker with just brief access to the ICP scanner’s memory card could determine how individual voters voted (*id.*).

Dr. Halderman expounds on the specific nature of these vulnerabilities at great length in his 2021 Report. As a brief example, related to his first identified vulnerability — QR code alteration — Dr. Halderman explains how attackers could cause the BMDs to print ballots with QR codes encoded with selections different from a voter’s actual selections while leaving the human-readable text summary

unchanged, making alterations difficult to detect. (*Id.* at 14.) As a second example, related to his second, third, and fourth vulnerabilities — all of which concern malware — Dr. Halderman explains that attackers could install malware on the machines either by physical access (for example, by inserting a USB device) or by remote access (for example, by modifying election definition files that election workers copy to all BMDs before each election). (*Id.* at 32, 39, 49.) Although these are just two general examples, and the Court does not delve further into Dr. Halderman’s extensive vulnerability findings, the Court’s review of his full Report indicates, at least at this juncture, that appropriate evidence and expert analysis have been provided to support the seven outlined vulnerability findings.

Besides addressing the specific vulnerabilities of the BMD machines and related equipment, Dr. Halderman’s Report further opines on the broader risks flowing from those vulnerabilities. For example, Dr. Halderman explains that the risk of ballot manipulation is far greater when BMDs are used for *all* in-person voters, like they are in Georgia, versus when BMDs are only used for a *small fraction* of voters, e.g., voters who may require special accommodations. (*Id.* at 16.) When only a small subset of voters uses BMDs, even if an attacker changes every BMD ballot, the attack could only affect the outcome of contests with very narrow margins, which means that “successful fraud would usually require cheating on such a large fraction of BMD ballots that it would likely be discovered.” (*Id.*) Thus, jurisdictions where only a fraction of voters use BMDs are a less appealing target than states where most voters use BMDs. (*Id.*)

Additionally, Dr. Halderman highlights the growing risk of an attack on a Georgia election by various adversaries — such as domestic political actors, election insiders, voters, and hostile foreign governments. (*Id.* at 12.) Regarding foreign governments, Dr. Halderman explains that Russia targeted Georgia’s election infrastructure during the 2016 election and states that other “hostile foreign governments” might attempt to hack Georgia’s election system to change election outcomes. (*Id.*)²⁶ Regarding domestic political actors, Dr. Halderman opines that politically motivated hackers might seek to alter individual votes and change the outcome of an election. (*Id.* at 13.)

Dr. Halderman also opines that election insiders and ordinary voters could be recruited by domestic political actors or hostile sophisticated foreign nations to attack Georgia’s voting system by, for instance, implanting malware. (*Id.* at 13.) This opinion is consistent with a 2019 report from the Senate Select Committee on Intelligence (“SSCI report”) (cited above in Section IV.2.a.), which recounted hearings revealing Russian interference efforts with the 2016 election and voting process. (8/15/19 PI Order, Doc. 579 at 40–42.) As the Court noted in its 2019 PI Order:

The July 2019 SSCI report noted that Russian government cyber actors engaged in operations to scan the election-related state infrastructure of all fifty states and conducted research on “general election-related web pages, voter ID information, election system software, and election service companies” and that Russian operatives

²⁶ Dr. Halderman also explained that nation-state actors are among the most technically sophisticated and well-resourced adversaries facing Georgia’s election system, and are particularly difficult to defend against. (*Id.*)

were able to penetrate the voter registration databases and access voter registration data from Illinois and at least one other state.

(*Id.* at 42) (citing SSCI Report at 8, 22.) The Court further noted that:

Counties in Georgia were targeted as well. In July 2018, Special Counsel Robert Mueller released an indictment that alleged that a Russian operative “visited the websites of certain counties in Georgia, Florida, and Iowa” on or about October 28, 2016.

(*Id.* at 42) (citing Georgia Official Election Bulletin, Doc. 471-7 at ECF 3.)

These final observations unfortunately resonate with later developments involving electronic distribution of Coffee County’s election data and software, to, among others, unauthorized domestic political representatives and retained contract software consultants. And critically, because the Coffee County election software and voting data was uploaded to the internet, it was left open to manipulation by other non-authorized individuals, organizations, or adversary nations.

While Dr. Halderman acknowledges in the overview of his Report that “[a]ll voting systems face cybersecurity risks,” and that “there is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats,” he also emphasizes that not all voting systems are equally vulnerable. (*Id.* at 4.) Based on the seven particular vulnerabilities he identified, Dr. Halderman provides the following “Main Conclusions” in his Report:

- **The ICX BMDs are not sufficiently secured** against technical compromise to withstand vote-altering attacks by bad actors who are likely to attack future elections in Georgia. . . .

- The ICX BMDs can be compromised to the same extent and as or more easily than the AccuVote TS and TS-X DREs they replaced. . . .
- Despite the addition of a paper trail, ICX **malware can still change individual votes and most election outcomes without detection** . . . Although outcome-changing fraud conducted in this manner could be detected by a risk-limiting audit, Georgia requires a risk-limiting audit of only one contest every two years,²⁷ so the vast majority of elections and contests have no such assurance. And even the most robust risk-limiting audit can only assess an election outcome; it cannot evaluate whether individual votes counted as intended. . . .
- The ICX's vulnerabilities also make it possible for an **attacker to compromise the auditability of the ballots**, by altering both the QR codes and the human readable text. Such cheating could not be detected by an [risk-limiting audit] or a hand count, since all records of the voter's intent would be wrong. . . .
- **Using vulnerable ICX BMDs for all in-person voters, as Georgia does, greatly magnifies the security risks** compared to jurisdictions that use hand-marked paper ballots but provide BMDs to voter upon request. . . .
- The critical vulnerabilities in the ICX — and the wide variety of lesser but still serious security issues — indicate that **it was developed without sufficient attention to security** during design, software engineering, and testing. . . . [I]t would be extremely difficult to retrofit security into a system that was not initially produced with such a process.

(*Id.* at 6–7) (emphases added). The Court has provided this highly condensed summary of Dr. Halderman's 66-page, single-spaced Report (excluding the exhibits attached to the Report) — which contains significantly more information.

²⁷ In 2023, the Georgia legislature modified the requirements for auditing. O.C.G.A. § 21-2-498(b).

2. U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) Corroborates Dr. Halderman's Findings

The next big development that occurred in the case involves the CISA²⁸ Advisory. Approximately six weeks after filing the Halderman Report, the Curling Plaintiffs asked the Court to authorize them to share the Report with CISA so that it could review the vulnerabilities identified by Dr. Halderman and begin its own vulnerability disclosure process, if appropriate. (*See* Aug. 10, 2021 Hr'g Tr., Doc. 1160 p. 83.) The Court authorized the Curling Plaintiffs to share Dr. Halderman's Report with CISA. (*See* Feb. 2, 2022 Hr'g Tr., Doc. 1307 at p. 30.) After its review, CISA issued and posted its public ICS Advisory addressing "Vulnerabilities Affecting Dominion Voting Systems ImageCast X" on June 3, 2022. (CISA Advisory, Doc. 1631-46.)

In its Advisory, CISA confirmed many of the vulnerabilities identified by Dr. Halderman but also noted that it found (as of 6/3/2022) "no evidence that these vulnerabilities have been exploited in any elections." (*Id.* at ECF 2.) CISA also stated that, to exploit these vulnerabilities, a malicious actor would need to have physical access to either a BMD or the EMS, or otherwise have the ability to modify

²⁸ CISA is an operational component of the U.S. Department of Homeland Security. As DHS's website explains, in part: "The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure." Further, "[t]he agency has two primary operational functions. First, CISA is the operational lead for federal cybersecurity, charged with protecting and defending federal civilian executive branch networks," and "[s]econd, CISA is the national coordinator for critical infrastructure security and resilience, working with partners across government and industry to protect and defend the nation's critical infrastructure." *See* <https://www.dhs.gov/topics/cybersecurity>, (last visited September 9, 2023).

files before they are uploaded to the BMDs. (*See id.*) At the time of the report, CISA was unaware of the Coffee County breach, which began in January 2021.

In addition to confirming specific vulnerabilities, CISA detailed a series of mitigation steps that jurisdictions using Dominion’s voting system should follow to prevent vulnerabilities from being exploited. (*Id.* at ECF 3–4.) On this mitigation front, CISA noted that “[m]any of these mitigations are already typically standard practice in jurisdictions where these devices are in use and can be enhanced to further guard against exploitation of these vulnerabilities.” (*Id.* at ECF 2.) According to CISA, Dominion represented that many vulnerabilities at issue had already been addressed in later versions of its software. (*Id.* at ECF 4.) CISA therefore recommended that jurisdictions using Dominion’s software “[c]ontact Dominion Voting Systems to determine which software and/or firmware updates need to be applied.” (*Id.*) Despite this, a number of critical software updates related to the operation of Dominion’s software and equipment have not been purchased or installed in Georgia as of the date of this Order.

Besides using up-to-date software and firmware, CISA also recommended other mitigation steps. These mitigation steps included ensuring that:

- “all affected devices are physically protected before, during, and after voting”;
- “ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks”;
- “carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all affected devices, including on connected devices such as printers and connecting cables”; and

- “all ImageCast X devices are subjected to rigorous pre- and post-election testing.”

(*Id.*) As another mitigation step, CISA recommended that jurisdictions “[c]onduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records.” (*Id.*) It emphasized that — in jurisdictions like Georgia, where votes are counted based on the selections contained within a QR code — these audits “are especially crucial to detect attacks . . . a barcode is manipulated to be tabulated inconsistently with the human-readable portion of the paper ballot.” (*Id.*) CISA added that, as an alternative to the QR code-based system, “the ImageCast X provides the configuration option to produce ballots that do not print barcodes for tabulation.” (*Id.*)²⁹ To date, no evidence has been presented that the State Defendants have implemented CISA’s recommended mitigation steps.

3. Fortalice’s 2021 Technical Assessment Identifies Several Vulnerabilities in the Secretary of State’s Internal and External Systems

The next relevant development concerns a 2021 assessment conducted by Fortalice, a forensic services company retained by the State Defendants.³⁰ Unlike Dr. Halderman, who focused his assessment on the potential vulnerabilities of the

²⁹ As previously noted, the Court indicated in its 2020 PI Order that it “cannot fathom why, post-election, the State and Dominion would not at least be moving toward consideration of the software upgrade option.” (10/11/20 PI Order, Doc. 964 at 146.)

³⁰ The Secretary of State’s Office hired Fortalice to perform cybersecurity assessments initially in 2017 and 2018. The head of Fortalice, Theresa Payton, testified at the August 2019 hearing regarding the work that her computer forensics firm had done as of that date and which of their findings required follow-up remedial action. Fortalice’s review at that time — as in the years thereafter — focused on the forensic security issues facing the Secretary of State’s Office at large, rather than on the Elections Division in particular, or on election security in county election offices across the state. (*See* 8/15/19 PI Order, Doc. 579 at 75–89.)

election equipment, operations, and Dominion software, Fortalice focused its assessment on potential vulnerabilities in the Secretary of State's Office's external, public-facing websites and its internal network. (Fortalice 2021 Report, Doc. 1635-28 at ECF 5.)

After testing for weaknesses in the Secretary of State's Office's external and internal systems, Fortalice identified eight specific vulnerabilities, and provided a rating of high, medium, or low risk for each vulnerability — with four vulnerabilities rated high risk, three rated medium risk, and one rated low risk. (*Id.* at ECF 8.) These vulnerabilities involved, among other things, issues with insecure password storage or repeated/weak passwords, overly broad file sharing accessibility within the internal system, and failure to maintain software patches. (*Id.*) Besides identifying these vulnerabilities, Fortalice also provided low- to no-cost recommendations on how the State could address each vulnerability. (*Id.*)

Despite this Fortalice Report, there is no evidence in the record (one way or another) that the State Defendants have remediated these risks, or what corrective measures, if any, have been taken. There is also no evidence reflecting whether Fortalice was ever asked to conduct any other security assessments of the Elections Division or review its handling of cybersecurity issues arising in county election offices across Georgia.³¹

³¹ According to the Secretary of State's Office Chief Information Officer with responsibility for election cybersecurity and technology, Merritt Beaver, Fortalice stopped providing written reports of its technical assessments to the Secretary's Office and began providing its reports over phone because the written reports had been "taken out of context by the public." (Feb. 2, 2022 Rule

4. Breach of Voting System in Coffee County By Various Political Actors and Hired Consultants (1/7/21 and Onward)

Perhaps the most significant development since the 2020 PI phase of this case involves the breach of the voting system in Coffee County, Georgia, which began on January 7, 2021, the day after the attack on the Capitol in Washington, D.C. Plaintiffs brought this revelation to the Court's attention when the parties were on the verge of completing discovery in 2022. The events of the Coffee County breach and the ensuing developments are complex and sprawling. The Court provides a short summary before outlining the events in more detail in the following sections.

Broadly speaking, the Coffee County breach involved various individuals and entities (1) providing and gaining unauthorized access to Coffee County voting equipment, data, and software over the course of multiple dates; (2) copying, downloading, and imaging the County's equipment, data, and software; (3) uploading and sharing that data and software on the internet via a file-sharing website; and (4) further distributing physical copies of forensic voting material downloaded from Coffee County. (Declaration of Kevin Skoglund ("Skoglund Decl."), Doc. 1635-44 ¶ 9.) These acts were committed by a number of individuals and entities including, among many others, the Coffee County Republican Party

30(b)(6) Dep. of Merritt Beaver, Doc. 1370-2 pp. 71–72.) Beaver is the Chief Information Officer for both the Georgia Secretary of State and Insurance and Safety Fire Commission. (*Id.* p. 94.)

Chair (Cathy Latham³²), the former Coffee County Election Supervisor (Misty Hampton), a private bail bondsman politically active in challenging the aftermath of the 2020 Presidential election (Scott Hall), employees of an Atlanta-based forensics firm (SullivanStrickler), attorneys who retained SullivanStrickler (including Sidney Powell), a hired security consultant (Jeffrey Lenberg), and the CEO of a company called Cyber Ninjas (Doug Logan). (*Id.* ¶¶ 9, 15, 22, 59.) Plaintiffs’ experts have opined that the above-described copying and broad distribution of voting system data and software materially increases the risk that a future Georgia election will be attacked — especially because all 159 counties in Georgia use the same voting system software and system configurations. (*See, e.g.*, Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 6.b.)

In this case, the State Defendants claim that they first learned of the Coffee County breach in February 2022 (over a year after the breach began), during a deposition of Gabriel Sterling, the Chief Operating Officer of the SOS’s Office, which was conducted for this case.³³ (*See* Joint Discovery Statement, Doc. 1360 at 5.) During Sterling’s deposition, counsel for the Coalition Plaintiff played a recording of a March 2021³⁴ phone conversation between the Coalition’s Executive

³² Ms. Latham testified before the Georgia Legislature on December 30, 2020 regarding her concerns about the Dominion voting system and the election. (*See* Georgia Senate Election Law Study Subcommittee of the Standing Senate Judiciary Committee: December 30, 2020 Meeting Minutes, Docs. 1360-2, 1360-3.)

³³ The State Defendants contend that they would have known about the unauthorized access earlier if Plaintiffs had disclosed the recording to them sooner.

³⁴ Mr. Hall’s call seems to have occurred in March 2021. (*See* Feb. 24, 2022 Dep. of Gabriel Sterling, Doc. 1370-5 p. 260) (where Plaintiffs’ counsel represents that call took place in March of 2021).

Director, Marilyn Marks, and bail bondsman Scott Hall, which Hall had initiated.³⁵ On the call, Mr. Hall explained how he and others were present at the Coffee County election office on January 7, 2021 when a forensic team from SullivanStrickler performed a review of the election equipment and data systems; began copying the election software, voter ballots, and data; and examined and handled the voting equipment. (Recording of Hall/Marks Call, Doc. 1363; Partial Tr. of Marks/Hall Call, Doc. 1364.)

Although the State Defendants assert that they did not learn of the Coffee County breach until Mr. Sterling's February 2022 deposition, the State was aware of, and was in fact investigating, other election-related concerns in Coffee County from December of 2020 through the spring of 2021, some of which were at least in part connected to the breach. These investigations are discussed at length in Subsection f. Having provided this overview, the Court dives into significantly more detail below.³⁶

³⁵ No evidence has been presented that Mr. Hall had a prior existing connection with Ms. Marks.

³⁶ The Court's recounting of the facts in this section are largely drawn from declarations submitted by Plaintiffs' cybersecurity experts, Kevin Skoglund and Dr. Alex Halderman. In preparation for his testimony, Mr. Skoglund reviewed Coffee County Election Office surveillance footage as well as forensic images from Coffee County's EMS server and other election equipment. (Declaration of Kevin Skoglund ("Skoglund Decl."), Doc. 1635-44 ¶ 5; PSAMF, Doc. 1626 ¶ 314; Defs.' Resp. to PSAMF, Doc. 1653 ¶ 314.) Dr. Halderman also reviewed forensic images from Coffee County's EMS server and other election equipment. (PSAMF, Doc. 1626 ¶ 314.) The events captured in the surveillance footage discussed in this Order were discovered after one volunteer for the Coalition, Paschal McKibben, spent approximately 177 hours reviewing video footage related to the breach in Coffee County. (See 2/10/23 Decl. of Marilyn Marks, Doc. 1618 ¶¶ 25-26.)

a. Physical Access to Coffee County's Election Equipment and Copying of Software and Data Begins on January 7, 2021

On January 7, 2021, four employees from an Atlanta-based forensics firm, SullivanStrickler, travelled to the Coffee County Election Office and used forensic tools and techniques to copy election software and data over a seven-hour period. (Skoglund Decl., Doc. 1635-44 ¶¶ 9.b, 24.) SullivanStrickler's work was directed by Scott Hall, Cathy Latham, and Misty Hampton, and was paid for by Sidney Powell, a lawyer associated with Donald Trump. (Sept. 2, 2022 SullivanStrickler Rule 30(b)(6) Dep. of Dean Felicetti, Doc. 1489-2 pp. 75, 146.)³⁷

During their seven hours in the Coffee County Election Office on January 7, SullivanStrickler's team copied and forensically imaged a significant number of election equipment items. Importantly, the Coalition Plaintiffs' expert explained that a "forensic image is a copy of a physical data storage device which copies every data bit exactly as it exists on the device," and can even include previously deleted data. (Skoglund Decl., Doc. 1635-44 ¶ 41.) Therefore, such a forensic image "has significantly more fidelity to the original device than a copy made by dragging directories and files to a new device." (*Id.*) The particular items forensically imaged and collected by the SullivanStrickler team on January 7, 2021 included:

- **the Coffee County's Election Management System server ("EMS")** as it existed on January 7, 2021 (*id.* ¶ 42). Data on the server

³⁷ Besides the four SullivanStrickler employees, Hall, Latham, and Hampton, other individuals present throughout the day included: Coffee County Election Board Member Eric Chaney; a former Coffee County Election Board Member named Ed Voyles; a data analyst named Alex Cruce; and an assistant to Ms. Hampton. (Skoglund Decl., Doc. 1635-44 ¶¶ 21, 22.)

included the Windows installation and configuration, the Dominion EMS software, and *all election data present on the server* as of that date (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 12.a);

- **the Dominion ICC central-count scanner** (which is used to record vote selections from absentee ballots) as it existed on January 7, 2021 (Skoglund Decl., Doc. 1635-44 ¶ 44). Data on the ICC scanner hard drive included the Windows installation and configuration as well as the Dominion ICC software (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 12.b);
- **18 CompactFlash memory cards** used with Dominion ImageCast Precinct (“ICP”) scanners/tabulators from Coffee County as they existed on January 7, 2021 (Skoglund Decl., Doc. 1635-44 ¶ 46). These 18 memory cards contained data from the 2021 runoff election, as well as residual ballot images from the 2020 General Election (*id.* ¶ 49);
- **A Mobile Ballot Printing laptop** as it existed on January 7, 2021 (*id.* ¶ 53). Data on this laptop’s hard drive included Windows installation and configuration and the Dominion mobile ballot production software (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 12.c);
- **7 USB drives** as they existed on January 7, 2021 (Skoglund Decl., Doc. 1635-44 ¶ 50). Six of these USB drives contained election projects (such as data about ballots, contests, candidates, etc., *see id.* ¶ 51), and one appears to have been used to install election definition files on Coffee County’s BMD machines (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 12.g.)

Besides forensically imaging items, the SullivanStrickler team also copied the following items on January 7, 2021:

- **the Android application software** or ICX application installation files for Georgia’s BMDs (which is responsible for most of the BMDs functionality) (*id.* ¶ 12.d);
- **a version of the application software for the Dominion ICP scanners** (the scanners used to count ballots produced by BMD machines) (*id.* ¶ 12.e);

- partial, but not complete, **data from 20 PollPad devices** (*id.* ¶ 12.h);
- **election-related reports** for the 2020 General Election and 2021 Run-off Election (Skoglund Decl., Doc. 1635-44 ¶ 53); and
- **scanned images of ballots** from the 2021 Run-Off election (*id.*).

Of all of the data forensically imaged and copied, Dr. Halderman opined that the ICX Android application software/installation files contain “the most important information that someone would need to develop attacks against the” BMDs. (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 15.)

b. Election Software and Data is Uploaded and Accessed from January 2021 Onward

After collecting the aforementioned software and data, the SullivanStrickler team (specifically an employee named Paul Maggio), uploaded all the acquired information onto ShareFile, an internet-based file storage and sharing site, that could be accessed by specific users (“the Coffee County ShareFile”).³⁸ (Skoglund Decl., Doc. 1635-44 ¶¶ 56–57.) An activity log from ShareFile indicates that at least five or six individuals downloaded the Coffee County data during January and February 2021, and at least some of these individuals shared their ShareFile credentials with others. (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 13; Skoglund Decl., Doc. 1635-44 ¶ 75.) In addition, some of these individuals may

³⁸ Administrators of a ShareFile account “can grant users permission to access certain directories.” (Skoglund Decl., Doc. 1635-44 ¶ 56.) Users can then “upload and download files in those directories through a public website.” (*Id.*)

have further distributed the election software and data. (Skoglund Decl., Doc. 1635-44 ¶ 75.)

One individual who downloaded the Coffee County data, Doug Logan of CyberNinjas,³⁹ testified that he then converted the forensic images of the server and the central-count scanner into “virtual machines” and uploaded those virtual machines onto the Coffee County ShareFile in January 2021. (See Logan Dep., Doc. 1612 at pp. 125–126.)⁴⁰ Logan explained that “converting [forensic images] [in]to a virtual machine allows you to potentially, you know, boot up the device and be able to utilize it like it was the computer in order to take a look at the way the things operate, and more closely examine it like it was a local system you were using.” (*Id.* at pp. 125–126.) In other words, “Logan uploaded a new version of the forensic image that could be used more easily for analysis.” (Skoglund Decl., Doc. 1635-44 ¶ 63.)

All in all, Plaintiffs contend that the user activity of SullivanStrickler’s ShareFile site shows that at least 10 individuals “downloaded data from locations as far-reaching as California, Kansas, England, and Italy.” (Curling Opp. Brief, Doc. 1625 at 17) (citing Download Records, Doc. 1635-37.) This trail, of course,

³⁹ Logan’s Cyber Ninjas firm performed a widely criticized, allegedly partisan, audit of the Arizona presidential election that was rejected by Maricopa County and Arizona Secretary of State’s Office election officials. See <https://www.nbcnews.com/politics/politics-news/cyber-ninjas-company-led-arizona-gop-election-audit-shutting-down-n1287145> (published January 6, 2022), (last visited October 15, 2023). The Cyber Ninjas business announced its closing at the time of the conclusion of the Arizona election audit review process.

⁴⁰ According to Dr. Halderman, a “virtual machine simulates a running computer system and allows an analyst to interactively operate a copy of the computer—logging into Windows, running applications, etc.—without modifying the forensic image or the original computer.” (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 22.)

does not disclose who else these individuals — or other entities in possession of the downloaded data — transferred that election software and voting data to, or the chain reaction flowing from those transfers.

c. Continued Physical Access to Coffee County Elections Equipment on January 18–19, 2021

On January 18, 2021, four individuals — consultant Jeffrey Lenberg, Doug Logan (of Cyber Ninjas), Elections Supervisor Misty Hampton, and her daughter — were present in the Coffee County Elections Office for a four-hour period. (Skoglund Decl., Doc. 1635-44 ¶ 94.) Security cameras revealed that, during that timeframe, Hampton and her daughter retrieved election equipment including blank ballots and an ICP scanner (the scanner used to count ballots produced by the BMDs). (*Id.* ¶¶ 95–96.) The next day, the same group returned for approximately nine hours, during which time they handled a second ICP scanner and roll of paper tape used for printing ICP election results. (*Id.* ¶ 96.)

In his deposition, consultant Jeffrey Lenberg testified that the group went to Coffee County because they believed there was “a major anomaly,” and they wanted to “run testing on the equipment” to test their theory. (Lenberg Dep., Doc. 1613 pp. 110–112.) When they showed up, Misty Hampton “got on her BMD” and “created a number of ballots,” some for Biden and some for Trump, so that the group could run “ICP testing” of the ICP scanner. (*Id.*) They also retrieved blank ballots to fill out by hand to run testing of the ICC scanner (used for paper ballots).

(*Id.*) Together, the group ran “batch after batch after batch” and “were running the same ballots over and over and over and over.” (*Id.*)

The Coalition Plaintiffs’ expert, Mr. Skoglund, explained that a review of the ICC scanner log files (files that log information about user activity) showed that, on January 18, the ICC scanner scanned 772 ballots in 6 batches, and on January 19, scanned 5,084 ballots in 33 batches. (Skoglund Decl., Doc. 1635-44 ¶ 108) (further noting that later on January 19, “the log file recorded a noticeable increase in scanner errors and batches that halted on ambiguous marks on a ballot.”) Unlike the ICC scanners (used for the paper ballots), it is not clear what exactly the group did with the ICP scanners. (*Id.* ¶ 110.) However, Lenberg testified that Hampton opened up one of the two ICP scanners to look inside the equipment. (Lenberg Dep., Doc. 1613 p. 289.)

In addition to “running tests” on the scanners, Lenberg also testified that he changed the dates on the ICC scanners and the EMS server to assess whether there had been a potential hack. (*Id.* pp. 117–118) (explaining that Lenberg thought that a “bad actor” might “potentially use the date as a trigger,” and so he thought “let’s reverse the date on the machine. [He] asked Misty to do that, to set the date back to November 5th, so that it would be within a reasonable period of time of the election in case that was being used as a trigger mechanism.”)

According to Plaintiffs’ expert Mr. Skoglund, Lenberg and Logan’s activities were organized by two attorneys (James Penrose and attorney Charles Bundren). (See Skoglund Decl., Doc. 1635-44 ¶¶ 9.e; 16.) At least one of these attorneys

(Penrose) was associated with Sidney Powell and her organization Defending the Republic. (Lenberg Dep., Doc. 1613 p. 32.)

d. Continued Physical Access to Coffee County Elections Equipment from January 25–29, 2021

The next unauthorized physical access to, and handling of, Coffee County election equipment occurred over the course of five straight days, between January 25–29, 2021. On January 25, three of the same individuals — consultant Lenberg, Elections Supervisor Hampton, and her daughter — returned to the Coffee County Elections Office where they accessed an ICP scanner, blank ballots, a BMD, and a printer. (Skoglund Decl., Doc. 1635-44 ¶ 118.) Mr. Skogland’s subsequent review of the EMS server revealed that, on this date, the election event software was used to program memory cards and USB drives to be used with a BMD and scanner. (*Id.* ¶ 120.) Additionally, log files show that more than 500 ballots were scanned in 25 batches. (*Id.* ¶ 122.)

On January 26, Lenberg returned to the Coffee County Elections Office, and, at some point during his visit, an inspector with the Secretary of State Investigations Division arrived to speak with Hampton about voting matters that the state was investigating in Coffee County. (*Id.* ¶ 123.) Lenberg left Hampton’s office and did not return until the State’s inspector left. (*Id.*)

On January 27, Lenberg returned to the Coffee County Election Office once again but left after 23 minutes. (*Id.* ¶ 125.) That same day, consultant Lenberg, consistent with his testimony that he believed there to be “an anomaly,” (Lenberg

Dep., Doc. 1613 pp. 110–112), submitted an Open Records Request to Coffee County, stating that he was “doing independent research to help verify the accuracy of the 2020 General Election” and requested copies of the ICP scanner result tapes and the batch and tally sheets for the full hand recount of the 2020 General Election. (Skoglund Decl., Doc. 1635-44 ¶ 127.)

On January 28, Lenberg returned to the Coffee County Election Office, this time to pick up a thumb drive from Hampton containing a compressed file named “Coffee CF.zip,” which included data from the 2021 Run-off Election. (*Id.* ¶¶ 129–30.) On January 29, Lenberg returned to the Coffee County Election Office, during which time Hampton accessed and showed him a PollPad, demonstrated how it worked, and showed him how it could be connected to the internet. (Lenberg Dep., Doc. 1613 pp. 71–72.)

e. Arrangements Made for Forensic Voting Material Downloaded from Coffee County to be Further Distributed to Entities and Persons Outside the State

Coffee County election equipment and data was further compromised in April 2021. That month, Paul Maggio (an employee of SullivanStrickler) had a disk drive — which included all forensic material copied at the Coffee County Elections Office — sent to consultant Lenberg and private investigator Michael Lynch⁴¹ in Michigan. (Skoglund Decl., Doc. 1635-44 ¶¶ 76–81.) Maggio did this at the request

⁴¹ Michael Lynch is a private investigator who Lenberg testified worked closely with Stephanie Lambert. (*Id.* ¶ 79; Lenberg Dep., Doc. 1613 p. 103:9–16.)

of attorneys Penrose and Lambert; Maggio invoiced Lambert for the work. (*Id.* ¶ 77.) Upon receipt, Lenberg made a copy of the disk drive. (*Id.* ¶ 81.)

Michigan-based attorney Lambert took the mailed disk drive and provided it to a digital security firm, CyFIR, so that CyFIR could forensically examine the Coffee County election software and data. (*Id.* ¶¶ 84–85.) The founder of CyFIR (Ben Cotton) later testified that he accessed the SullivanStrickler Coffee County ShareFile and downloaded Coffee County files stored there on or around June 11–12, 2021. (*Id.* ¶ 87.) Cotton further testified that the data was still saved on his computer at the time of his deposition on August 25, 2022. (*Id.*)

In light of the above events — spanning from January 7, 2021 to the present — it is, according to Dr. Halderman, currently impossible to determine the number of people or entities that have copies of the Coffee County software and data. (Nov. 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 13.) Indeed, according to Dr. Halderman, anyone who has a copy of the software and data has the level of access sufficient to discover several vulnerabilities in the EMS sever and the ICC scanner, craft malware to exploit those vulnerabilities, and test the malware against copies of the EMS server and ICC scanner running in virtual machines. (*Id.* ¶ 14.) Thus, because of these “outside group(s) and individuals copying and distribution of the proprietary software that operates Georgia’s election system and specific system configurations” the risk that a future Georgia election will be attacked has “materially increased.” (*Id.* ¶ 6.b.)

f. The State Defendants' Response to Events in Coffee County

The State Defendants contend that they were not aware of the Coffee County breach that began in January 2021 until February 2022. This is despite the fact that the State was aware of, and was even investigating, other election-related issues in Coffee County during the same timeframe. Some of these issues were connected to the Coffee County breach. These election-related issues include: the Secretary of State's investigations into Hampton's December 2020 posting of a YouTube video about manipulation of Dominion software; the State's investigation into Coffee County's handling of the 2020 presidential election recount; and the Secretary of State's communications with the new replacement Coffee County Elections Supervisor about EMS server passwords no longer working and the related discovery of a business card for Doug Logan's Cyber Ninjas on the base of Misty Hampton's computer. The Court outlines the State's awareness of, and response to, these events now.

The first election-related issue that the State Defendants knew of involves a YouTube video posted by Coffee County Elections Supervisor Hampton in December of 2020. (See Hampton YouTube Video Screenshots and Video Link, Doc. 1630-22.) In the video, Hampton discusses various ways that Dominion's election software could allegedly be manipulated.⁴² (Secretary of State Report of Investigation, Doc. 1630-26 at 2.) The video shows Hampton sitting in front of a

⁴² (See Hampton YouTube Video Screenshots and Video Link, Doc. 1630-22 at 3) (exhibit includes video link: <https://www.youtube.com/watch?v=46CAKyyObls&t=16s>.)

computer, with what appears to be a note with a password written on it taped to the bottom of the computer screen. (Nov. 22, 2022 Decl. of J. Alex Halderman, Doc. 1635-19 ¶ 54.) In reviewing the video, Dr. Halderman surmised that the password displayed was the login password for the Coffee County EMS server. (*Id.* ¶ 55.)⁴³ The Secretary of State's Office was aware of this video and opened an investigation as a result of its posting. (Secretary of State Report of Investigation, Doc. 1630-26 at 2.)

The Misty Hampton YouTube video was not the only election issue the Secretary of State's Office was investigating in Coffee County. On December 9, 2020, the Secretary of State's Office opened an investigation into Coffee County's handling of the 2020 presidential election recount and recount procedures after receiving a letter from the Coffee County Board of Elections and Registration stating that it could not certify its recount. (*See* SOS Press Release, Doc. 1360-4.) During this timeframe, the State was also investigating a third issue in Coffee County related to an absentee ballot request from a voter. (Secretary of State Report of Investigation, Doc. 1630-26 at 2–3.)

The Report of Investigation covering these three issues indicates that the Secretary of State's Office sent investigators to Coffee County on multiple dates to look into these events. (*Id.*) Surveillance footage confirms this, showing that

⁴³ Dr. Halderman opined that, although the EMS server password was changed in December 2020, shortly after the YouTube video emerged, the password that appears on the note was (at the time of his declaration) still being used as the password for the ICC scanner workstation, which apparently had the same password as the EMS server. (*Id.* ¶¶ 55–56.)

investigators visited Coffee County on three dates in winter 2020–2021: December 11, 2020; January 20, 2021; and January 26, 2021. (Pls.’ Statement of Additional Facts, Doc. 1637 ¶ 337.) Notably, one of these visits occurred on the same date (January 26, 2021) that consultant Jeffrey Lenberg was present in the Coffee County Elections Office. (*Id.* ¶ 338.) Ms. Hampton also testified that, at some point after she resigned in February 2021,⁴⁴ an investigator from the Secretary of State’s Office contacted her to discuss an unrelated issue about a Coffee County voting activist who filed a complaint about her treatment by the Coffee County Elections Office after she allegedly touched the voting machines during the 2020 election. (Nov. 11, 2022 Dep. of Misty Hampton, Doc. 1610 pp. 227–29, 237.)

Months later, in September 2021, the Secretary of State’s Office issued its summary of findings related to the investigation into these three issues, including the YouTube video incident. (Secretary of State Report of Investigation, Doc. 1630-26.) This Report of Investigation does not reference any events of the Coffee County breach that began on January 7, 2021 — or system irregularities that might have been suggested by the evidence collected during the investigations.

⁴⁴ Ms. Hampton was forced to resign from her position as Coffee County Elections Supervisor in February 2021, though the precise reason for her termination remains unclear. For example, in Gabe Sterling’s deposition, he stated that he understood Ms. Hampton was terminated for her alleged falsification of time records. (Sterling Dep., Doc. 1370-5 p. 265). But Ms. Hampton’s testified at her deposition that it was her belief that she was forced to resign because of the video of people coming in and out of the Elections Office, and that “the State and Dominion was coming down on Coffee County.” (Hampton Dep., Doc. 1610 pp. 142–143.) Hampton ultimately was replaced by James Barnes in April 2021. (July 20, 2022 Dep. of James A. Barnes, Jr., Doc. 1630-17 p. 85.)

Besides the three issues addressed in the Report of Investigation, the Secretary of State's Office, *in April and May 2021*, also received a phone call and later emails from the new Elections Supervisor in Coffee County, James Barnes. In his call and emails, Barnes indicated that passwords for Coffee County's EMS server no longer worked and that a business card for the Doug Logan's Cyber Ninjas business was found at the base of Hampton's computer. (May 7, 2021 Email from James Barnes to Chris Harvey, Doc. 1631-27 at 3-4.) Specifically, a few weeks into his tenure, in April 2021, Barnes discovered that the EMS server and ICC scanner passwords no longer worked. (July 20, 2022 Dep. of James A. Barnes, Jr., Doc. 1630-17 pp. 107-08.) Upon making this discovery, Barnes notified the Center for Elections Systems by phone. (*Id.*) The discovery that the passwords did not work further concerned Barnes because he had seen a copy of Doug Logan's Cyber Ninjas business card at the base of Ms. Hampton's computer. (May 7, 2021 Email from James Barnes to Chris Harvey, Doc. 1631-27 at 3-4.) In light of this additional concern, Barnes emailed the Secretary of State's Director of Elections, Chris Harvey, about his discovery of the Cyber Ninja's business card. (July 20, 2022 Dep. of James A. Barnes, Jr., Doc. 1630-17 p. 108; May 7, 2021 Email from James Barnes to Chris Harvey, Doc. 1631-27.) Barnes later explained that part of the reason he contacted the Secretary of State's Office was because he was concerned that the server was potentially compromised, and he thought there could be a connection between Hampton's association with the Cyber Ninjas and the EMS and ICC passwords not working. (July 20, 2022 Dep. of James Barnes, Doc. 1630-17 p. 162)

(stating “part of my concern was that, you know, potentially somebody had done something to that server”).

Four days after receiving Mr. Barnes’s email (on May 11, 2021), the Director of Elections (Chris Harvey) responded, noting:

James,

Thanks for sending this. I think it might be prudent to see if there has been any contact between the person on the card and anyone in your office and/or if they have had any access to any of your equipment.

I have let our investigations Division and CES know, and they might follow up with you. Let me know if you have questions or concerns.

(May 11, 2021 Email from Chris Harvey to James Barnes, Doc. 1631-27 at 1.) Ultimately, after two individuals from CES followed up with Mr. Barnes, the Secretary of State’s Office replaced the Coffee County EMS server and the computer attached to the ICC around June 8, 2021. (Pls.’ Statement of Additional Facts, Doc. 1637 ¶ 359.) No other equipment was replaced and no other follow-up appears to have occurred at the time.

Nearly a year later, in mid-March 2022, the Secretary of State’s Office opened an investigation into the Coffee County breach some weeks or months after Mr. Sterling had listened to the recording of the call between Scott Hall and Marks at his deposition. (Aug. 2, 2022 Decl. of Ryan Germany, Doc. 1444-1 ¶ 21.) Despite this knowledge, the State Defendants continued to deny that there was any cause for concern. For example, in a Discovery Statement that was submitted to the Court on April 6, 2022, the State Defendants represented that, “State Defendants are

investigating several issues related to Coffee County but at this time do not believe any of them demonstrate a breach of actual equipment.” (Joint Discovery Statement, Doc. 1360 at 5.) And several weeks later, the Secretary of State’s COO Gabriel Sterling went a step further, claiming at a public forum that the breach “didn’t happen.” (See Carter Center Panel Video, Doc. 1633-17) (“So we are still dealing with that here and we still have to prove negatives in all these cases. It’s similar across the board. But like, we had claims . . . even recently there was people saying: ‘We went to Coffee County. We imaged everything.’ There’s no evidence of any of that. It didn’t happen.”). When he was later asked about Mr. Sterling’s comments in a September 2022 interview, Secretary Raffensperger said that the reason why Mr. Sterling thought nothing had happened was because the individuals the Secretary of State’s investigators had interviewed had not been truthful. (See 11Alive Article, Doc. 1633-16.) Raffensperger simultaneously maintained that the Secretary’s office learned about the breach early on and had been continuing to investigate the matter.⁴⁵ (*Id.*) The Secretary of State’s General Counsel, Ryan Germany further explained, “[g]iven the type of allegations and the fact that the person asserting these claims had made many other allegations that were not factually supported regarding the 2020 election, our office determined to

⁴⁵ The article Plaintiffs reference notes that there were several inconsistencies in Secretary Raffensperger’s remarks. He initially stated that the Secretary of State’s Office knew of the breach in January of 2021, but within minutes of so stating, an aide corrected the Secretary of State’s response off camera and offered May of 2021 as the correct date. (See 11Alive Article, Doc. 1633-16.) The article then adds that afterwards “a representative with the Secretary of State’s Office clarified that the office did not know about or began investigating Coffee County until July 2022.” (*Id.*)

first undertake a forensic evaluation of the server at issue . . . ” (Aug. 2, 2022 Decl. of Ryan Germany, Doc. 1444-1 ¶ 22.)

In attempting to undertake such a forensic evaluation, the Secretary of State’s Office, in spring 2022, contacted Dominion to attempt to gain access to the Coffee County EMS. However, Dominion was unsuccessful. (*Id.* ¶ 23; see Oct. 12, 2022 30(b)(6) Dep. of Gabriel Sterling, Doc. 1635-27 pp. 212–15.) After Dominion’s efforts failed, the Secretary of State’s Office brought in a consulting expert with prior GBI experience to attempt to access to the server. (Aug. 2, 2022 Decl. of Ryan Germany, Doc. 1444-1 ¶ 25.) This consulting expert, Jim Persinger, ultimately gained access to the server on or around July 5, 2022. (Nov. 10, 2022 Decl. of James Persinger, Doc. 1635-40 ¶ 22.)

About a month later, the Secretary of State’s Office referred the matter to GBI on August 2, 2022 via a letter from the Secretary of State’s Deputy General Counsel, Steven Ellis, to GBI Director Vic Reynolds. (Letter from Steven Ellis to Vic Reynolds, Doc. 1633-33 at 2.) The letter stated, in relevant part,

Our office is investigating allegations that unauthorized individuals claim to have accessed various election materials and equipment in Coffee County, Georgia under case number SEB2020-250. During the course of our investigation, we have identified evidence that indicates the possibility of the commission of cyber- and computer-related crimes. . . .

As a result, I write to request the GBI exercise its authority to assist agencies with investigations to assist the Secretary of State’s office in its investigation of possible election- and cyber-related crimes in Coffee County, Georgia.

(*Id.*) The GBI opened an investigation into the breach, which remained ongoing at the time Defendants filed their Motions for Summary Judgment on January 9, 2023. (*See* List of SOS Investigations, Doc. 1633-18.)

Nearly two months after this August 2, 2022 request to GBI — and possibly more than a year and a half after information regarding the breach became evident — the Secretary of State’s Office replaced the remaining equipment in the Coffee County Election Office on September 26, 2022. (SOS 9/23/22 Announcement, Doc. 1632-45; Notice of Filing Re: Coffee County Equipment, Doc. 1632-46.) The equipment replaced included all BMDs; all printers that were used with the BMDs; and all the precinct scanners, flash cards, and thumb drives; but not the EMS server and ICC scanner, as those had been replaced in June 2021. (Notice of Filing Re: Coffee County Equipment, Doc. 1632-46; Oct. 12, 2022 30(b)(6) Dep. of Gabriel Sterling, Doc. 1635-27 pp. 159–61.) The replaced EMS Server and ICC Scanner, though, would have been subject to any possible malware potentially transferred by the above-mentioned voting equipment in the time before such voting equipment was replaced in September 2022.

Although the equipment was replaced, thus far, none of it has been examined for malware. (*Id.* p. 152; Pls.’ Resp. to State Defs.’ SUMF, Doc. 1638 ¶ 437.)⁴⁶ According to published news accounts, the GBI investigation was completed and turned over to the Georgia Attorney General’s Office on or about September 7, 2023. Also, on August 14, 2023, the Fulton Count DA’s office

⁴⁶ The parties dispute the significance of this fact.

unveiled a criminal indictment of Cathy Latham, Scott Hall, Misty Hampton, Sidney Powell, former President Donald J. Trump, and others related to their conduct in Coffee County. *See Georgia v. Trump et al.*, 23SC188947 (Fulton Cty. Super. Ct. Aug. 14, 2023).⁴⁷

F. Current Procedural Posture

On January 9, 2023, State Defendants and the Fulton County Defendants filed Motions for Summary Judgment on all claims. (Docs. 1567, 1568, 1571.) In the following weeks, the parties submitted over 350 pages of briefing and thousands of pages of exhibits in support of their positions. The Court held oral argument on Defendants' Motions on May 2, 2023. Since that time, the parties have also filed several notices of supplemental authority identifying new factual and legal developments for the Court's consideration. The Court also held two lengthy status conferences with counsel in the months following oral argument. (*See* 6/16/23 Minute Entry, Doc. 1683; 9/1/23 Minute Entry, Doc. 1695.) With this comprehensive evidentiary framing, the Court now moves to its analysis of the legal issues.

⁴⁷ Latham, Hall, Hampton, Powell, were charged with violation of the Georgia Racketeer Influenced and Corrupt Organizations ("RICO") Act, conspiracy to commit election fraud, conspiracy: to commit computer theft, to commit computer trespass, to commit computer invasion of privacy, and to defraud the State. Latham was also charged with impersonating a public officer, forgery in the first degree, false statements and writings, and criminal attempt to commit filing false documents. *See Georgia v. Trump et al.*, 23SC188947 (Fulton Cty. Super. Ct. Aug. 14, 2023). At this point, Hall, Powell, and two other defendants in the case (Jenna Ellis and Kenneth Chesebro) have entered guilty pleas.

V. Discussion

Defendants contend that they are entitled to summary judgment both on jurisdictional grounds and on the merits. Broadly speaking, the State Defendants argue that the Court lacks jurisdiction over Plaintiffs' claims because Plaintiffs lack standing to challenge the current BMD system and because any remaining claims related to the old DRE system are now moot. The Fulton County Defendants separately argue that Plaintiffs' claims against them should fail because they are not proper defendants in this matter.

On the merits, Defendants argue that they are entitled to summary judgment on all claims because Plaintiffs fail to present any evidence that the BMD system imposes a burden on their constitutional rights, and, even if they had, those burdens would be insufficient to override the State's interest in implementing the existing BMD system. (State Defs.' MSJ., Doc. 1568-1 at 2–3) (arguing that “the State's interest in an orderly election system more than justifies the choice of that equipment,” and in any case, “Georgia's choice of equipment rests squarely within the constitutional authority of the state legislature.”)

In Plaintiffs' view, they have presented sufficient evidence to establish standing, or, “[a]t the very least, material facts pertaining to standing are disputed and must await resolution at trial.” (Coalition Pls.' Opp'n, Doc. 1624 at 79.) With respect to the merits, Plaintiffs argue that “material facts are disputed as to the existence and magnitude of the burdens” imposed by the current election system, and that the “task of weighing th[ose] burdens” should be left for trial. (*Id.*)

Before diving in, the Court notes that many of the parties' jurisdictional arguments substantially overlap with their merits arguments. For example, Defendants argument that Plaintiffs lack standing because their asserted harm is speculative overlaps with their argument on the merits that Plaintiffs fail to establish that the current BMD system burdens their constitutional rights. There is thus some repetition of the relevant arguments and evidence.

In resolving the pending motions, the Court begins by addressing threshold questions of standing and mootness. After finding that Plaintiffs have, viewing the facts in their favor, provided sufficient evidence to support standing, the Court then considers the merits of Plaintiffs' constitutional claims. After addressing the merits of the fundamental right to vote and equal protection claims, the Court addresses the remaining components of the Coalition Plaintiffs' claims related to ballot secrecy, scanner settings, and paper backups of the pollbooks.

A. Standing

Defendants first assert that because all Plaintiffs lack Article III standing to pursue their claims, summary judgment should be granted for lack of subject matter jurisdiction. *See Kennedy v. Floridian Hotel, Inc.*, 998 F.3d 1221, 1229 (11th Cir. 2021) (cleaned up) ("The standing doctrine stems directly from Article III's case or controversy requirement and implicates our subject matter jurisdiction."). Plaintiffs counter that numerous outstanding factual issues preclude the Court from granting Defendants summary judgment on standing grounds.

A plaintiff must demonstrate standing “for each claim he seeks to press and for each form of relief that is sought.” *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 581 U.S. 433, 439 (2017) (quoting *Davis v. Fed. Election Comm’n*, 554 U.S. 724, 734 (2008)). The question of whether a plaintiff has standing is separate from the question of whether the plaintiff will ultimately prevail on the merits of his asserted claims. See *Wooden v. Bd. of Regents of Univ. Sys. of Ga.*, 247 F.3d 1262, 1280 (11th Cir. 2001). But courts will often have to consider certain aspects of the merits of a plaintiff’s claims to make the threshold standing determination. See *Warth*, 422 U.S. at 500–01 (1975) (citations omitted).

A plaintiff must establish three elements to have Article III standing. First, “the plaintiff must have suffered an ‘injury in fact.’” *United States v. Hays*, 515 U.S. 737, 743 (1995) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). To satisfy this requirement, a plaintiff must show “an invasion of a legally protected interest that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.” *Id.* at 743 (quoting *Lujan*, 504 U.S. at 560); see *Fla. State Conference of NAACP v. Browning*, 522 F.3d 1153, 1159 (11th Cir. 2008). Second, the injury must have been fairly traceable to the defendant’s challenged actions rather than to “the independent action of some third party not before the court.” *Lujan*, 504 U.S. at 560 (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976)); see *Browning*, 522 F.3d at 1159. Third, the plaintiff’s injury, or threat of injury, must be “likely . . . redressed by a favorable decision.”

Lujan, 504 U.S. at 561 (citing *Simon*, 426 U.S. at 38); see *Browning*, 522 F.3d at 1159.

Here, each set of Plaintiffs asserts that they have standing. The Curling Plaintiffs argue that they each have individual standing. The Coalition Plaintiffs argue that their individual Plaintiffs have individual standing and that their organizational Plaintiff, CGG, has both organizational standing in its own right and associational standing on behalf of its members. See *Warth*, 422 U.S. at 511 (stating that an organization may have standing both “in its own right to seek judicial relief from injury to itself” and to “assert the rights of its members, at least so long as the challenged infractions adversely affect its members’ associational ties”). The Court begins by addressing whether CGG has organizational standing.

1. CGG’s Standing

“An organization can establish standing in two ways: (1) through its members (i.e., associational standing) and (2) through its own injury in fact that satisfies the traceability and redressability elements” (i.e., standing in its own right). *Ga. Ass’n of Latino Elected Officials, Inc. (“GALEO”) v. Gwinnett Cnty. Bd. of Registration & Elections*, 36 F.4th 1100, 1114 (2022). The Coalition Plaintiffs assert that CGG has both associational standing and standing in its own right. The Court first determines whether CGG has standing in its own right.

To assess whether an organizational plaintiff has standing in its own right, the Court conducts “the same inquiry as in the case of an individual.” See *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 378–79 (1982). It must demonstrate “(1)

an injury in fact that (2) is fairly traceable to the challenged action of the defendant and (3) is likely to be redressed by a favorable decision.” *See Jacobson v. Florida*, 974 F.3d 1236, 1245 (11th Cir. 2020) (citing *Lujan*, 504 U.S. 555, 560–61). The Court addresses each element in turn.

a. Injury in Fact

It is well established that “an organization can establish its own injury in fact under a diversion of resources theory.” *See GALEO*, 36 F.4th at 1114 (citing *Jacobson*, 974 F.3d at 1249–50); *Fair Fight Action, Inc. v. Raffensperger*, 634 F. Supp. 3d 1128, 1177 (N.D. Ga. 2022). “Under this theory, an organization has standing ‘if the defendant’s illegal acts impair its ability to engage in its projects by forcing the organization to divert resources to counteract those illegal acts.’” *GALEO*, 36 F.4th at 1114 (quoting *Jacobson*, 974 F.3d at 1250). But this requires the organizational plaintiff to “explain where it would have to ‘divert resources away *from* in order to spend additional resources on combating’ the effects of the defendant’s alleged conduct.” *GALEO*, 36 F.4th at 1114 (quoting *Jacobson*, 974 F.3d at 1250) (emphasis original); *see, e.g., Common Cause/Ga. v. Billups* (“*Billups*”), 554 F.3d 1340, 1350 (11th Cir. 2009) (finding an organization had standing because it diverted “resources from its regular activities to educate and assist voters in complying with” a challenged photo ID law); *Browning*, 522 F.3d at 1164–66 (finding an organization had standing because it diverted resources from performing voter registration drives and election monitoring to “educating

volunteers and voters on compliance with [the challenged law] and to resolving the problem of voters left off the registration rolls on election day”).

Additionally, an organization seeking to establish standing under a diversion-of-resources theory “cannot do so by inflicting harm on itself to address its members’ ‘fears of hypothetical future harm that is not certainly impending.’” *City of S. Miami v. Governor*, 65 F.4th 631, 638 (11th Cir. 2023) (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 416 (2013)). Thus, “[t]o prove injury in fact based on an organization’s diversion of resources to protect individuals from harm, the organizational plaintiff must prove *both* that it has diverted its resources *and* that the injury to the identifiable community that the organization seeks to protect is itself a legally cognizable Article III injury that is closely connected to the diversion.” *City of Miami*, 65 F.4th at 638–39 (emphasis original). Such harm “must be concrete and imminent.” *Id.* at 639.

Plaintiffs contend that the Eleventh Circuit has already confirmed that CGG has organizational standing through a diversion-of-resources theory in this case. Specifically, they point to the Eleventh Circuit’s decision regarding the State Defendants’ appeal of the Court’s paper backup and scanner setting Orders. *See Curling*, 50 F.4th at 1121. There, one argument the State Defendants raised before the Eleventh Circuit was that this Court lacked jurisdiction to hear the case because the Coalition Plaintiffs lacked standing. The Eleventh Circuit squarely rejected that argument. It explained:

We have recognized that voting advocacy organizations like the Coalition have standing to sue when a policy will force them “to divert personnel and time to educating volunteers and voters” and to resolving problems that the policy presents “on election day.” *Florida State Conf. of the NAACP v. Browning*, 522 F.3d 1153, 1165–66 (11th Cir. 2008); see also, e.g., *Georgia Ass’n of Latino Elected Offs., Inc., v. Gwinnett Cnty. Bd. of Registration & Elections*, 36 F.4th 1100, 1114 (11th Cir. 2022). Because the Coalition credibly made that assertion, the district court had jurisdiction to hear the Coalition’s and its members’ requests for injunctive relief.⁴⁸

Id. Thus, the Eleventh Circuit “confirmed” that CGG had standing at that point in the case’s litigation. See *id.*

In light of this finding by the Eleventh Circuit, Plaintiffs contend that the “law-of-the-case doctrine” requires the Court to treat the issue of standing as already decided. This doctrine holds that “an issue decided at one stage of a case is binding at later stages of the same case.” *Schiavo ex rel. Schindler v. Schiavo*, 403 F.3d 1289, 1291 (11th Cir. 2005) (citation omitted); see also *A.A. Profiles, Inc. v. City of Fort Lauderdale*, 253 F.3d 576, 582 (11th Cir. 2001) (“Generally, the law of the case doctrine requires a court to follow what has been explicitly or by necessary implication decided by a prior appellate decision.”). Although there are “a few

⁴⁸ During the oral argument for the appeal, several Judges on the Eleventh Circuit panel appeared highly skeptical of the State Defendants’ arguments that CGG lacked organizational standing. Several minutes into defense counsel’s argument, one of the panelists, Judge Grant inquired, “what do you identify specifically as different between this set of this organizational plaintiff versus the dozens that we have found have standing for in other election cases?” Oral Argument at 04:24–04:35. *Curling v. Raffensperger*, 50 F.4th 1114 (11th Cir. 2022) (No. 20-13730), https://www.ca11.uscourts.gov/oral-argument-recordings?title=20-13730&field_oral_case_name_value=&field_oral_argument_date_value%5Bvalue%5D%5Byear%5D=&field_oral_argument_date_value%5Bvalue%5D%5Bmonth%5D=. Another one of the panelists, Judge Luck, advised the Coalition Plaintiffs’ counsel right at the start of his response time that he should focus his arguments on the merits instead of standing. *Id.* at 14:33–14:48. And just a few minutes later, he reiterated to counsel, “I think you have standing.” *Id.* at 19:15–19:16. Shortly thereafter, Judge Grant stated, “We are not talking about standing. Standing is over.” *Id.* at 20:36–20:38.

discreet exceptions” to application of the law-of-the-case doctrine, *see Schiavo*, 403 F.3d at 1292, Defendants have not established that any apply here. Thus, the law-of-the-case doctrine requires the Court follow what was previously decided by the Eleventh Circuit. *See A.A. Profiles, Inc.*, 253 F.3d at 582.

But the State Defendants contend that the issue of CGG’s standing was not conclusively decided in the Eleventh Circuit’s 2022 opinion. They argue that because the 2022 opinion concerned Plaintiffs’ preliminary injunction motions, and the Coalition Plaintiffs must now clear a higher evidentiary bar to establish standing at summary judgment, the issue is once again before the Court. On this issue, the Court acknowledges that CGG must establish that it has standing “with the manner and degree of evidence required at the successive stages of the litigation.” *Jacobson*, 974 F.3d at 1245 (quoting *Lujan*, 504 U.S. at 561). But as discussed below, after review of the relevant legal and evidentiary factors, the Court finds that CGG has continued to satisfy that burden for purposes of summary judgment.

i. CGG Diverted Resources to Counteract Defendants’ Alleged Unlawful Conduct

To begin, Plaintiffs have shown that CGG has diverted resources to combat Defendants’ alleged unlawful conduct. *See City of Miami*, 65 F.4th at 638. CGG’s executive director, Marilyn Marks, has provided both oral and written testimony explaining the numerous ways in which Defendants’ continued use of the BMD system and refusal to institute needed changes has strained CGG’s resources and

resulted in CGG and its members diverting their resources away from other projects. In addition to challenging Defendants' use of the BMD system through this litigation, Marks stated that CGG has engaged in the following activities in response to Defendants' conduct: lobbying state and county lawmakers about BMD-related issues, including by "promoting effective audits"; attending SAFE Commission⁴⁹ meetings; educating its own members about both "the problems with the BMDs" and the "necessity for audits"; and proposing rules to the SEB addressing these same topics. (Mar. 17, 2022 30(b)(6) Dep. of Marilyn Marks, Doc. 1569-25 pp. 158–59.) In a February 12, 2021 declaration, Marks provided a laundry list of projects that CGG had diverted its attention from as a consequence of its work on this case and related issues surrounding the State's use of the BMD system. Marks explained:

Some examples include: inability to participate in the EAC's current process of accepting comments on the controversial pending Voluntary Voting System Standards; sharply reducing active involvement in Election Verification Network (a national organization of election experts); declining most speaking invitations on the topic of election security; ceased active involvement in State Audit Working Group (experts focused on developing election auditing standards); ceased activity in weekly meetings of Election Cybersecurity Working Group (a group proposing VVSG standards to NIST); ceased work in on-going drive-up voting project CGG initiated in North Carolina; became inactive in working with other North Carolina election transparency groups on voter education and transparency efforts in Wake County; reduced collaboration with North Carolina NAACP on voter education on election security; stopped participation in meetings of the North Carolina State Board of Elections; stopped

⁴⁹ According to the Georgia Secretary of State's website, the Secure, Accessible & Fair Elections ("SAFE") Commission was established by former Secretary of State Brian Kemp in 2018 "to study options for Georgia's next voting system." *Election Safeguards*, Georgia Secretary of State Brad Raffensperger, <https://sos.ga.gov/page/elections-safeguards> (last visited July 11, 2023).

participation in Charlotte-Mecklenburg Board of Elections meetings; lacked resources to provide requested consulting support for another non-profit organization's North Carolina state court case on ballot marking devices; abandoned CGG's plans to file a lawsuit in North Carolina against the use of ballot marking devices; deferred plans to file a lawsuit in North Carolina on the violations of secret ballot laws; limiting CGG's involvement in the current effort to educate the New York State Board of Elections on the problems in using Ballot Marking Devices; declining request of Colorado members to help educate the Boulder Colorado City Council on problems with Instant Runoff Voting; declining the request of Georgia members to conduct voter education or author an opinion piece on the difficulties with Ranked Choice Voting; cancel plans for candidate forum on election security prior to the November election; cancel plans to conduct a meeting regarding Georgia needed election law changes with a group of Georgia lawmakers; delayed preparation of education materials for Georgia election officials regarding HB270; and failing to keep our website, fundraising efforts and donor communications current.

(2/12/21 Suppl. Decl. of Marilyn Marks, Doc. 1071-2 ¶ 10.)

In a February 2023 declaration, Marks stated that these types of activities “continue to be activities CGG resources have been diverted from in order to challenge the conduct of the Defendants with respect to the use of the BMD system.” (2/10/23 Decl. of Marilyn Marks, Doc. 1618 ¶ 35.)⁵⁰ She added that in past years, CGG prepared drafts of potential legislation and met with lawmakers during the Georgia General Assembly's legislative session about issues related to

⁵⁰ The State Defendants argue that the Court should not consider Ms. Marks's declaration testimony about how CGG diverted its resources because it contradicts her prior deposition testimony in which — at least according to the State Defendants — she failed to explain how CGG diverted its resources. They rely on the Eleventh Circuit's decision in *Van T. Junkins & Associates v. U.S. Industries, Inc.*, 736 F.2d 656 (11th Cir. 1984), where it stated, “When a party has given clear answers to unambiguous questions which negate the existence of any genuine issue of material fact, that party cannot thereafter create such an issue with an affidavit that merely contradicts, without explanation, previously given clear testimony,” *id.* at 657. Contrary to the State Defendants' suggestion, Marks's declaration is not a sham affidavit as it is fully consistent with her prior testimony about the myriad ways in which CGG has diverted its resources in response to Defendants' conduct. (See 2/12/21 Suppl. Decl. of Marilyn Marks, Doc. 1071-2 ¶ 10.)

government transparency and oversight. (*Id.* ¶ 31.) But she explained that “[t]he demands of challenging the BMD system have curtailed most legislative lobbying activity for CGG projects.” (*Id.*)

Marks also identified one CGG volunteer in particular, Paschal McKibben, who she claimed spent approximately 177 hours since last fall reviewing video surveillance footage of the unauthorized access to the voting system in Coffee County, Georgia, which had prevented him from engaging in other CGG projects. (*Id.* ¶¶ 25–26.) Marks explained,

The hours that Mr. McKibben has spent on the Coffee County video were hours taken away from his ability and capacity to undertake video creation and editing projects he has volunteered to do for CGG. He has volunteered to help create training and educational videos, but because of our efforts to challenge the BMD voting system, he is unable to engage in those activities and our team is unable to organize such efforts. Those efforts would include educational videos on our Accurate Count Project with Scrutineers, and our desired Ranked Choice Voting educational efforts, advising municipal officials on conducting their own elections, among other topics.

(*Id.* ¶ 26.) Marks also noted, “Mr. McKibben has been a poll observer for CGG, but was unable to serve except in a limited capacity during the 2022 general election and runoff because of the priority and time urgency of the Coffee County video project.” (*Id.* ¶ 27.) And although Mr. McKibben “volunteered to participate as a CGG monitor in [CGG’s] joint Scrutineers ‘Accurate Count’ project to create an audit trail of Election Night Reporting results,” Marks stated that she “asked him to prioritize the Coffee County video review instead.” (*Id.* ¶ 28.)

In short, just as the Eleventh Circuit previously concluded, Plaintiffs have “credibly” asserted that CGG has diverted resources in response to Defendants’

conduct. *See Curling*, 50 F.4th at 1121. Plaintiffs have provided sufficient evidence that CGG’s “actual ability to conduct specific projects” not only will be, but in fact, has been “frustrated.” *See Browning*, 522 F.3d at 1166. “Such concrete and demonstrable injury to the organization’s activities — with the consequent drain on the organization’s resources — constitutes far more than simply a setback to the organization’s abstract social interests[.]” *Havens Realty Corp.*, 455 U.S. at 379. “This effect on the operations of the organization[is] a ‘concrete injury’ sufficient to confer standing.” *Billups*, 554 F.3d at 1350 (citing *Browning*, 522 F.3d at 1165–66).

None of Defendants’ arguments to the contrary are persuasive. First, relying on *Equal Rights Center v. Post Properties, Inc.*, 633 F.3d 1136 (D.C. Cir. 2011), the State Defendants argue that CGG’s claimed diversion is really just an increase in litigation expenses, and that CGG cannot claim to be injured simply by virtue of increases in such expenses.⁵¹ But as the court in *Equal Rights Center* observed, “While the diversion of resources to litigation or investigation in anticipation of

⁵¹ Counsel for the State Defendants raised a similar argument when addressing the issue of standing before the Eleventh Circuit. Evidently, the panel was not persuaded. When counsel for the State Defendants argued that CGG lacked standing because “the Coalition exists to litigate, that is its sole purpose,” Judge Luck responded, “so I looked at that and I know you make that argument but . . . at least in their allegations . . . it is alleged the executive director . . . would now have to spend efforts on education, instruction, and litigation as a result and otherwise would have done work on auditing and election reform efforts which is not litigation related so it seems to be — you might have a point if the only goal was litigation and that’s what they’re doing but this seems to be not that, this seems to be true diversion from at least something else.” Oral Argument at 04:39–05:16. *Curling v. Raffensperger*, 50 F.4th 1114 (11th Cir. 2022) (No. 20-13730), https://www.ca11.uscourts.gov/oral-argument-recordings?title=20-13730&field_oar_case_name_value=&field_oral_argument_date_value%5Bvalue%5D%5Byear%5D=&field_oral_argument_date_value%5Bvalue%5D%5Bmonth%5D=.

litigation does not constitute an injury in fact sufficient to support standing, [an organization's] alleged diversion of resources to programs designed to counteract the injury to its interest . . . *could* constitute such an injury.” *Id.* at 1140 (emphasis added). Here, the Coalition Plaintiffs have provided evidence of not only an increase in litigation expenses, but also a “diversion of resources to programs designed to counteract the injury to its interest” as a consequence of Defendants’ use of the BMD system. *See id.*

For example, CGG member Elizabeth Throop testified that she had previously helped prepare slideshows for webinars to educate the public on a wide range of topics ranging “from best practices for poll watchers, to the role of the State Election Board, to the importance of audits.” (2/7/23 Suppl. Decl. of Elizabeth Throop, Doc. 1596 ¶ 29.) But as a consequence of Defendants’ conduct, she explained that “CGG has had to devote considerable time in these presentations to covering problematic aspects of Georgia’s BMD voting system” instead of other topics. (*Id.*) Throop also stated that a “significant part” of her work for CGG in the past has been attending monthly meetings of the DeKalb Board of Registration and Elections (“BRE”) and presenting comments to the Board, but her recent comments have largely been focused on issues surrounding the BMD system’s voting equipment to the exclusion of other issues. (*Id.* ¶¶ 30–31.) She added, “CGG could be providing a great resource to the DeKalb BRE in many other aspects of election administration and transparency, but the challenge to the voting system diverts the time available to do so.” (*Id.*) Along these same lines,

Throop explained that she originally started poll watching for CGG “to find out whether voters are dissuaded or prevented from casting their votes due to challenging forms, notices, and ballots,” but that the need to focus on election security issues has prevented her from doing so. (*Id.* ¶ 8.)

As Ms. Throop’s testimony indicates, although CGG has clearly diverted significant resources from other projects to support its efforts to challenge the BMD system through this litigation, it has also devoted significant resources toward responding to the State’s use of the BMD system and educating citizens regarding their use of the election system through other avenues. (*See also* 2/7/23 Decl. of Jeanne Dufort, Doc. 1593 ¶ 52 (“The time spent on this litigation and other work challenging the BMD system greatly limits my ability to perform other work for CGG.”) (emphasis added); 2/7/23 Decl. of Aileen Nakamura, Doc. 1597 ¶ 88 (“[T]his litigation and CGG’s administrative and lobbying challenges to the BMD system have prevented, reduced or delayed much of CGG’s important work.”) (emphasis added)).

Second, the State Defendants argue that the Coalition Plaintiffs cannot establish standing on a diversion-of-resources theory because filing lawsuits and engaging in advocacy related to electronic voting and election administration is already a part of CGG’s organizational mission. In other words, they argue that the sorts of tasks that the Coalition Plaintiffs have performed in response to Defendants’ conduct are all tasks that CGG would have performed anyway. But as this Court recently explained, “a plaintiff may show a diversion of resources even

if it diverts from one activity aimed at achieving an organizational mission to a different activity aimed at that same mission.” *Fair Fight Action, Inc.*, 634 F. Supp. 3d at 1178 (collecting cases). “Similarly, when an organization diverts its resources to achieve its typical goal in a different or amplified manner, the organization may still gain standing.” *Id.* (citing *GALEO*, 36 F.4th at 1115, and *Browning*, 522 F.3d at 1166). Simply put, CGG can certainly establish a diversion of resources by showing that its expenditure of resources in response to Defendants’ conduct has limited its ability to pursue other projects that *also* advance its organizational mission. In such circumstances, “because plaintiffs cannot bring to bear limitless resources, their noneconomic goals will suffer.” *Browning*, 522 F.3d at 1166. The State Defendants’ arguments to the contrary are unpersuasive.

Next, the State Defendants argue that CGG has failed to provide sufficient evidence of a diversion of resources because it has kept inadequate records to substantiate its claims of diversion. For instance, the State Defendants note that CGG does not maintain a written annual budget or track volunteer time. (*See* State Defs.’ SUMF, Doc. 1569 ¶¶ 189, 199.) And they contend that these issues make it impossible to “quantify” any diverted volunteer time or determine “how much of [CGG’s] claimed diversion is due to this litigation and how much is due to other factors,” “which requests for assistance from other organizations it receives that are rejected due to a general lack of resources as opposed to its claims in this case,” or “when it diverts resources based on the actions of nonparty counties versus the actions of State Defendants.” (State Defs.’ Mot. for Summ. J., Doc. 1568-1 at 10–

11.) The Court understands the State Defendants’ concerns about the adequacy of CGG’s records. However, these supposed recordkeeping shortfalls do not erase the Coalition Plaintiffs’ credible assertions — made through sworn testimony, which the Eleventh Circuit has previously accepted as adequate — that CGG has diverted its resources in response to Defendants’ conduct. Given the solid and credible record that CGG has established, the Court does not view a higher degree of quantification as required at this stage of the proceedings.

As a fallback, the State Defendants argue that CGG has not been injured because it has used this case for fundraising purposes, meaning that it has financially *benefitted* from Defendants’ conduct instead of being harmed. To the Court’s knowledge, no court has ever accepted this novel argument. Regardless, CGG’s fundraising numbers would not eliminate its claimed injuries to its organizational and broader educational interests or its diversion of resources in response to the State’s conduct.

ii. CGG’s Diversion of Resources is Closely Connected to Efforts to Protect an Identifiable Community from a Nonspeculative, Cognizable Injury

In the cases where the Eleventh Circuit “has found standing based on a resource-diversion theory, the organizations pointed to a concrete harm to an identifiable community, not speculative fears of future harm.” *City of S. Miami*, 65 F.4th at 639. As *City of South Miami* explained:

In *Browning*, the organizations helped black voters comply with new voting rules that went into effect before an election. Those rules

applied to all voters, “forcing” the organizations to divert resources to educate these voters before the election. *Browning*, 522 F.3d at 1165. Similarly, in *Georgia Latino Alliance for Human Rights v. Governor of Georgia*, 691 F.3d 1250 (11th Cir. 2012), illegal immigrants faced a “credible threat of detention” under a new immigration law. *Id.* at 1258. So the law “forc[ed]” the organizations to divert resources to protect illegal immigrants from this imminent harm. *Id.* at 1260.

Id. Thus, to establish a resource-diversion injury, CGG “must present . . . concrete evidence to substantiate its fears,” rather than “commit resources based on mere conjecture about possible governmental actions.” *Id.* (cleaned up). At this juncture, the Court concludes that when all facts and inferences are construed in Plaintiffs’ favor, the robust record that they have put forth meets this burden for purposes of summary judgment and establishing standing.

Here, CGG has been forced to divert resources to protect its members’ right to have their votes counted as cast if they are required to vote on Georgia’s BMD voting system. The harm CGG fears is not based on unsupported or speculative notions, but is shown by testimony, documentation, and expert evidence. While Plaintiffs’ assembled record may not ultimately carry the day at trial, the Court deems it sufficient to establish the organization’s injury in fact at summary judgment.

First, an injury to CGG members’ right to have their votes counted as cast is a concrete, legally cognizable Article III injury. *See City of S. Miami*, 65 F.4th at 639–40. As the Supreme Court has recognized, “all qualified voters have a constitutionally protected right to vote,” and that right necessarily encompasses “the right of qualified voters within a state to cast their ballots *and have them*

counted.” *Reynolds v. Sims*, 377 U.S. 533, 554–54 (1964) (emphasis added). An injury to CGG members’ right to have their votes counted as cast is thus sufficiently concrete for standing purposes.

Second, this injury is closely connected to CGG’s diversion of resources. *See City of S. Miami*, 65 F.4th at 639–40. Construing the facts in their favor, Plaintiffs have put forth sufficient evidence to show that CGG has diverted its resources in response to the State Defendants’ selection, implementation, and maintenance of an election system that allegedly injures CGG members’ right to have their vote counted as cast.

Third, this injury is a sufficiently “imminent” threat to CGG members to survive summary judgment. *See City of S. Miami*, 65 F.4th at 638, 640. “While this standard does not require a plaintiff to show that it is ‘literally certain that the harms they identify will come about,’ it, at the very least, requires a showing that there is a ‘substantial risk’ that the harm will occur.” *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1338–39 (11th Cir. 2021) (quoting *Clapper*, 568 U.S. at 414 n.5). Construing all facts and inferences in Plaintiffs’ favor, as the Court must, this standard is satisfied here.

In the 2020 PI Order, the Court previously concluded that “[t]he substantial risks and long-run threats posed by Georgia’s BMD system, at least as currently configured and implemented, are evident.” (10/11/20 PI Order, Doc. 964 at 89.) The Court explained that Plaintiffs had “shown demonstrable evidence that the manner in which Defendants’ alleged mode of implementation of the BMD voting

system, logic and accuracy testing procedures, and audit protocols deprives them or puts them at imminent risk of deprivation of their fundamental right to cast an effective vote (i.e., a vote that is accurately counted).” (*Id.* at 79).

Among other evidence submitted with Plaintiffs’ preliminary injunction motion was Dr. Halderman’s testimony that, like the DRE system before it, the BMD system relied on out-of-date and vulnerable software. (*See* Aug. 19, 2020 Decl. of Alex Halderman, Doc. 785-2 ¶ 16.) Dr. Halderman explained that out-of-date software components present a security risk “because they frequently contain known, publicly documented vulnerabilities that have been corrected in later versions.” (*Id.* ¶ 17.) Accordingly, Dr. Halderman noted that Texas had refused to certify Dominion’s BMD system for use in its own elections based on a number of vulnerabilities that its examiners discovered in the system. (*Id.* ¶¶ 19–20.) And the PI Order recognized that Georgia was “the only state using the Dominion QR barcode-based BMD system statewide as the mandatory voting method for all in-person voters.” (10/11/20 PI Order, Doc. 964 at 15.)

Plaintiffs also presented significant evidence that both U.S. and Georgia elections are targets for hacking. Dr. Halderman testified that 18 states were the subject of cyberattacks in the 2016 election cycle, including Georgia. (Aug. 7, 2018 Decl. of Alex Halderman, Doc. 1628-1 ¶ 8.) And the Secretary of State’s own cybersecurity consultant, Theresa Payton of Fortalice — who previously served as the White House Chief Information Officer to President George W. Bush — agreed in her 2019 testimony that, before the 2018 midterm elections, she believed it was

a certainty that the elections would be targeted by hackers. (July 25, 2019 PI Hr’g Tr., Doc. 1628-29 at 206) (“Q. And going into the midterm elections of last year, you had grave concerns about election interference; correct? A. I did, yes. Still do. Q. In fact, going into the midterms of last year, you believe that one thing that we can be sure of is that a U.S. election will be hacked, no doubt about it; right? A. Yes.”)

These concerns were further corroborated by numerous government reports, some of which were discussed earlier in this Order. (*See* 8/15/19 PI Order, Doc. 579 at 35–42) (discussing, *e.g.*, Senate Select Committee on Intelligence Report). For example, Russia’s efforts to interfere with the 2016 election in “more than two dozen states” — including Georgia — were described in detail in the Mueller Report. (Aug. 19, 2020 Decl. of Alex Halderman, Doc. 785-2 ¶ 60.) In 2020, Dr. Halderman testified that the Mueller Report’s findings “leav[e] no doubt that Russia and other adversaries will strike again.” (*Id.* ¶ 60.) Likewise, the Office of the Director of National Intelligence “assessed that foreign threats to the 2020 election include[d] ‘ongoing and potential activity’ from Russia, China, and Iran,” and “conclude[d] that ‘[f]oreign efforts to influence or interfere with our elections are a direct threat to the fabric of our democracy.’” (Aug. 19, 2020 Decl. of Alex Halderman, Doc. 785-2 ¶ 62) (citing Office of the Director of National Intelligence, “Statement by NCSC Director William Evanina: Election Threat Update for the American Public” (Aug. 7, 2020)). Ultimately, Dr. Halderman opined that

“Georgia’s BMD-based election system does not achieve the level of security necessary to withstand an attack by these sophisticated adversaries.” (*Id.* ¶ 63.)

Based on this and other evidence, the Court concluded in the 2020 PI Order that the risks presented by the BMD system as it was then configured “are neither hypothetical nor remote under the current circumstances.” (10/11/20 PI Order, Doc. 964 at 145.) Instead, the Court found that “[t]he Plaintiffs’ national cybersecurity experts [had] convincingly present[ed] evidence that this is not a question of ‘might this actually ever happen?’ – but ‘when it will happen,’ especially if further protective measures are not taken.” (*Id.*)

Presently, Plaintiffs’ briefs opposing the pending Motions for Summary Judgment continue to rely on much of the same evidence that was before the Court in 2020. But importantly, Plaintiffs also offer new evidence, which has come to light since the Court’s 2020 PI Order. This new evidence further supports a finding that that the current configuration of Georgia’s BMD voting system and its mode of implementation and oversight by State Defendants present a substantial risk that CGG members’ votes will not be counted as cast.

Plaintiffs first point to Dr. Halderman’s July 2021 Expert Report, which demonstrates in painstaking detail how numerous attacks on Georgia’s election system could become a reality. It describes how a malicious actor could insert malware in a BMD device, alter audit logs, or even change votes by manipulating the QR codes containing a voters’ selections.

The Department of Homeland Security’s Cybersecurity & Infrastructure Security Agency corroborated many of the vulnerabilities identified in the Halderman Report,⁵² and indicated that these vulnerabilities should be mitigated as soon as possible. (CISA Advisory, Doc. 1631-46 at ECF 2.) But to date, the record evidence indicates that these vulnerabilities remain exposed. There is currently no evidence that the State has taken action to implement CISA’s recommended mitigation steps or otherwise responded to the vulnerabilities identified by Dr. Halderman. This is despite the fact that the Georgia Secretary of State’s Chief Operations Officer, Gabriel Sterling, agrees that these mitigation steps should be implemented.⁵³ (Oct. 12, 2022 30(b)(6) Dep. of Gabriel Sterling, Doc. 1562 p. 349.)

As was the case in 2020, Defendants fail to identify a single cybersecurity expert who endorses the current configuration of Georgia’s BMD system.⁵⁴ (*See* Feb. 11, 2022 30(b)(6) Dep. of Michael Barnes, Director of the Election Center Director for the Georgia Secretary of State, Doc. 1634-55 p. 296) (“Q. Can you identify one cybersecurity election expert that has endorsed the current Georgia

⁵² The State Defendants’ rebuttal expert on other related voting issues, Dr. Juan Gilbert, stated that he does not disagree with many of the technical failings identified by Dr. Halderman, (Oct. 29, 2021 Dep. of Juan Gilbert, Doc. 1635-17 pp. 217–45), and that Dr. Halderman was someone whom he would personally defer to on cybersecurity issues, (*id.* p. 144).

⁵³ However, Sterling clarified that he thought at least one of CISA’s recommendations was not technically feasible. (*See* Oct. 12, 2022 30(b)(6) Dep. of Gabriel Sterling, Doc. 1562 pp. 349–50.)

⁵⁴ The State Defendants’ expert, Dr. Gilbert, who specializes in *disability access issues* in the voting realm, indicated that he supported the State’s use of the BMD system, but acknowledges that he does not have Dr. Halderman’s background in cybersecurity. In addition, even though Dr. Gilbert represented that he thought a QR code-based system could be used, he stated, “if I had my choice, I would recommend not using them.” (Oct. 29, 2021 Dep. of Juan Gilbert, Doc. 1635-17 pp. 88–89.) In Dr. Gilbert’s view, eliminating the QR codes and switching to a full-face ballot system is “a solution that would get rid of a lot of these issues that we’re discussing.” (*Id.* at 88.)

system as a reliable voting system? A. I cannot.”).⁵⁵ Although Defendants cite a 2018 NAS report to argue that the scientific community recommends the use of BMDs, Plaintiffs have provided evidence that, since the report was issued, the scientific consensus surrounding the use of BMDs has changed. (*See* Pls.’ Resp. to State Defs.’ SUMF, Doc. 1638 ¶¶ 6, 427; *see also* Jan. 27, 2022 Dep. of Andrew Appel, Doc. 1553 p. 54.)⁵⁶

And critically, the ongoing revelations regarding the January 2021 Coffee County election equipment breach lend serious support to Plaintiffs’ argument that the current configuration of Georgia’s BMD voting system presents a substantial risk that CGG members’ votes will not be counted as cast. For some time, the State Defendants’ principal response to the issues raised in the 2021 Halderman Report was that Dr. Halderman was only able to simulate attacks on the State’s election system because he had unfettered access to the equipment. And they maintained that malicious actors would be unable to replicate any of those attacks because, unlike Dr. Halderman, they could not obtain access to the equipment. (*See, e.g.*, Feb. 24, 2022 30(b)(6) Dep. of Gabriel Sterling, Doc. 1634-53 pp. 70–71.) Plaintiffs persuasively contend that the Coffee County breach undermines that argument.

⁵⁵ The Court acknowledges that the MITRE Corporation performed a positive evaluation of the BMD system on behalf of Dominion, but as the Court previously explained, the Court cannot properly consider the MITRE Report for purposes of summary judgment. (*See* Doc. 1680 at 7) (“As the Defendants did not seek to make the MITRE Report available to the Plaintiffs during the discovery period prior to summary judgment briefing, the Court will not consider the MITRE report in connection with the summary judgment motion.”). The Court also notes that the MITRE Corporation never reviewed the BMD system’s *actual* implementation in Georgia or elsewhere or security practices used (or not used) in connection with this implementation.

⁵⁶ Whether this evidence is conclusive is another question.

(See Jan. 3, 2023 Dep. of Alex Halderman, Doc. 1570-8 p. 42) (stating that his takeaway from the Coffee County breach was that “the equipment is vulnerable” and outsiders could now obtain access to the election system to exploit vulnerabilities).

For his part, Dr. Halderman has testified that as a result of the Coffee County breach, “[t]he risk that a future Georgia election will be attacked materially increased,” particularly in light of the copying and wide geographic distribution of Dominion’s software.⁵⁷ (Nov. 22, 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 6.b.) Because copies of the Dominion software and voting system data from Coffee County were uploaded to the Internet, Dr. Halderman has opined that it is presently impossible to determine precisely how many people or entities have copies of the software and data, or will have copies in the future. (*Id.* ¶ 13.)

He further explained that this distribution of the proprietary Dominion software that operates Georgia’s election system (and data related to specific system configurations) arising from the Coffee County capers materially increases the risk that future Georgia elections will be attacked because “[t]echnical experts who analyze this data can discover vulnerabilities and develop means to exploit them.” (Nov. 22, 2022 Decl. of Alex Halderman, Doc. 1635-19 ¶ 6.b.) Critically, he noted that the heightened risk resulting from this breach “applies not only to

⁵⁷ Dr. Halderman had previously explained that “[s]oftware of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities” and “Nation-state attackers often discover and exploit novel vulnerabilities in complex software.” (Aug. 19, 2020 Decl. of Alex Halderman, Doc. 785-2 ¶ 15.)

Coffee County but to all other Georgia counties too, since counties throughout the state use the same Dominion software and the same or similar systems configurations.” (*Id.*)

In sum, Plaintiffs argue that the record shows that “[i]nherent design flaws, critical security failings, futile protective measures, advanced persistent threats, widely leaked voting software and data, extensive outsider access to the voting system in its operational environment, continued use of that equipment in subsequent elections, and persistent inaction by Defendants have *manifested* Plaintiffs’ concerns to a degree that seemed unthinkable years ago.” (Curling Pls.’ Opp’n, Doc. 1636 at 72) (emphasis in original).

Ultimately, after once again delving into the risks proposed by the current configuration of Georgia’s BMD voting system, the Court concludes that — for purposes of summary judgment — Plaintiffs have presented enough concrete evidence to support CGG’s concern and fear that there is a substantial risk of injury to its members’ right to have their votes counted as cast if they are required to vote on Georgia’s BMD system. *See City of S. Miami*, 65 F.4th at 639. Because Plaintiffs have sufficiently shown that CGG “has diverted its resources *and* that the injury to the identifiable community that the organization seeks to protect is itself a legally cognizable Article III injury that is closely connected to the diversion,” *see City of S. Miami*, 65 F.4th at 638–39, they have satisfied the injury-in-fact element for CGG’s standing.

b. Traceability

Having found that Plaintiffs presented sufficient evidence that CGG suffered an injury in fact, the Court now considers whether CGG's injury is traceable to the Defendants. To meet the standing traceability requirement, a plaintiff's claimed injuries "must be 'fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.'" *GALEO*, 36 F.4th at 1115 (quoting *Lujan*, 504 U.S. at 560–61). To satisfy this requirement, "a plaintiff need only demonstrate, as a matter of fact, 'a fairly traceable connection between the plaintiff's injury and the complained of conduct of the defendant.'" *GALEO*, 36 F.4th at 1116 (quoting *Charles H. Wesley Educ. Found., Inc. v. Cox*, 408 F.3d 1349, 1352 (11th Cir. 2005)) (emphasis omitted). And when the plaintiff is an organization, the plaintiff "need only allege a drain on [the] organization's resources that 'arises from the organization's need to counteract the defendants' asserted illegal practices.'" *GALEO*, 36 F.4th at 1116 (citing *Browning*, 522 F.3d at 1166) (internal quotation marks omitted).

Here, the Coalition Plaintiffs contend that each set of the Defendants has engaged in, and continues to engage in, unconstitutional conduct. According to Plaintiffs, examples of this include: (1) the Secretary of State's Office selecting and approving the BMD system and continuing to maintain that system for use in elections without providing necessary safeguards, patches, requisite monitoring and oversight, and other intervention actions, despite known vulnerabilities and deficiencies; (2) the SEB's promulgation of rules and regulations pertaining to the

implementation of that system, without taking essential corrective measures required to address the election system's cybersecurity, vulnerability, and in turn reliability; and (3) the Fulton County Defendants continuing to use that system for elections in Fulton County. Plaintiffs argue that this conduct has caused CGG to divert significant resources from other projects, as discussed above.

The State Defendants argue that, to the extent that CGG has been injured, those injuries are attributable to third parties, such as third-party hackers who Plaintiffs claim could exploit vulnerabilities in the State's election system or rogue election officials. In their Motion, the Fulton County Defendants argue that CGG's claimed injuries are not traceable to them either. Because the Secretary of State and Board are ultimately responsible for selecting and approving the State's election system — which must be the same in each county under state law — the Fulton County Defendants argue that they have no control over which election system is used and are thus not proper parties to this case. *See* O.C.G.A. § 21-2-300(a)(1) ("The equipment used for casting and counting votes in county, state, and federal elections *shall be the same in each county* in this state and shall be provided to each county by the state, *as determined by the Secretary of State.*") (emphasis added). For that reason, the Fulton County Defendants argue that to the extent CGG has been injured, those injuries are attributable only to the State Defendants and not to the Fulton County Defendants.

In response to the State Defendants, the Coalition Plaintiffs argue that CGG's injuries are attributable to the State Defendants, and not third parties,

because the State Defendants are the ones who are ultimately responsible for the election system’s security and its insecurity. Regarding the Fulton County Defendants, the Coalition Plaintiffs acknowledge that the State Defendants are ultimately responsible for selecting the statewide election system. But they argue that under a series of state statutory and regulatory provisions, Fulton County has the authority to utilize HMPBs on an emergency basis as an alternative to using the BMD system.⁵⁸ The Coalition Plaintiffs claim the substantial risk that using BMD system will violate voters’ constitutional rights qualifies as such an emergency. And they indicate that the Fulton County Defendants have refused to switch to a HMPB system on that basis, despite Plaintiffs’ requests.

Regarding the BMD-related claims, the Court finds that CGG satisfied the traceability requirement for its claims against the State Defendants based on evidence that the State Defendants’ conduct caused CGG’s alleged diversion of resources. *See GALEO*, 36 F.4th at 1116 (finding that traceability requirement was satisfied based on allegations that defendants “engaged in illegal conduct and that their conduct . . . caused GALEO to divert resources”). Specifically, the Court

⁵⁸ *See* O.C.G.A. § 21-2-281 (“In any primary or election in which the use of voting equipment is impossible or impracticable, for the reasons set out in Code Section 21-2-334, the primary or election may be conducted by paper ballot in the manner provided in Code Section 21-2-334.”); O.C.G.A. § 21-2-334 (“If a method of nomination or election for any candidate or office, or of voting on any question is prescribed by law, in which the use of voting machines is not possible or practicable, . . . the superintendent may arrange to have the voting for such candidates or offices or for such questions conducted by paper ballots.”); Ga. Comp. R. & Regs. 183-1-12-.11(2)(c)–(d) (“If an emergency situation makes utilizing the electronic ballot markers impossible or impracticable, as determined by the election superintendent, the poll officer shall issue the voter an emergency paper ballot that is to be filled out with a pen after verifying the identity of the voter and that the person is a registered voter of the precinct. . . . The existence of an emergency situation shall be in the discretion of the election supervisor.”).

concludes at this juncture that Plaintiffs have sufficiently shown that CGG’s diversion of resources is fairly traceable to the State Defendants’ selection, implementation, and maintenance of an election system that allegedly fails to provide CGG members with the means to cast a secure and effective vote. Although the evidence suggests that counties⁵⁹ are largely responsible for the physical security of their own voting equipment, the State Defendants are still responsible for selecting the voting system, maintaining its functionality, and for the overall responsibility for management and mitigation of any system cybersecurity vulnerabilities.⁶⁰

As the Court explained in its July 2020 Motion to Dismiss Order, the primary source of Plaintiffs’ claimed injuries is “Defendants’ implementation of an alleged unconstitutional voting system that is subject to the same demonstrated vulnerabilities as the DREs and that is not a voter-verifiable and auditable paper ballot system.” (7/30/20 MTD Order, Doc. 751 at 42.) Even if third parties unaffiliated with the State Defendants would have to act to exploit the claimed vulnerabilities before there was an effect on Plaintiffs’ votes, “the presence of

⁵⁹ (See Feb. 24, 2022 30(b)(6) Dep. of Gabriel Sterling, Doc. 1634-53 p. 118 (“Q. Who is responsible for securing elections, from the voting equipment to the servers to anything that touches the election system in Georgia? A. The counties. We are responsible for our E.M.S. [Election Management System] at our Center for Elections, but the counties secure the voting equipment and secure their E.M.S.s.”); Feb. 11, 2022 30(b)(6) Dep. of Michael Barnes, Doc. 1634-55 pp. 30–31 (stating that “[t]he counties are responsible for maintaining the security of their voting equipment.”)).

⁶⁰ (See Jan. 21, 2022 30(b)(6) Dep. of Derrick Gilstrap, Doc. 1630-13 p. 100 (“Q. Okay. So regarding cyber attack vulnerabilities, Fulton County looks to Georgia Secretary of State’s Office for guidance? Is that right? A. Yes, we do. Q. And they would look to the Secretary of State’s Office for guidance on implementing any measures that were necessary to address cyber attack vulnerabilities in Georgia’s election system. Is that also right? A. Yes.”))

multiple actors in a chain of events that lead to the plaintiff's injury does not mean that traceability is lacking with respect to the conduct of a particular defendant." *See Garcia-Bengochea*, 57 F.4th at 927. To the extent the State Defendants have failed to address known cybersecurity vulnerabilities on an ongoing and repeated basis, or to implement essential auditing protocols and practices, those acts and omissions would be plainly attributable to the State Defendants instead of third parties, and are therefore traceable the State Defendants. (*See* 7/30/20 MTD Order, Doc. 751 at 43.)

The Court reaches a different conclusion regarding the Fulton County Defendants. Unlike the State Defendants, the Fulton County Defendants are not responsible for the State's choice of voting system. Nor are the Fulton County Defendants responsible for any unmitigated vulnerabilities in the State voting system that may burden the voting rights of CGG members. Thus, to the extent CGG or any other Plaintiffs have any viable claims, the proper defendants for those claims are the State Defendants.

In an effort to show that CGG's claimed injuries are also attributable to the Fulton County Defendants, the Coalition Plaintiffs rely on the theory that Fulton County has the discretion to switch to a HMPB system in emergency situations, including those circumstances that would pragmatically undermine citizens' capacity to cast their votes reliably. Assuming that the violation of voters'

constitutional rights can qualify as such an emergency,⁶¹ the existence of such an emergency relative to the Coalition’s HMPB contention, as framed above, would still depend on Plaintiffs’ success on the merits of their claims against the State Defendants. Along these same lines, the Court has already rejected Plaintiffs’ prior request for mandamus relief to require the Fulton County Defendants to switch to a HMPB system because Plaintiffs had an alternative remedy: “injunctive relief in connection with the Plaintiffs’ constitutional claims pursuant to § 1983.” *See Curling v. Raffensperger*, 403 F. Supp. 3d 1311, 1348 (N.D. Ga. 2019). As far as the Court is concerned, the State Defendants are the only proper Defendants for those claims at this stage in the proceedings.⁶² Accordingly, Plaintiffs’ BMD-related claims are not traceable to the Fulton County Defendants, and Fulton County’s Motion for Summary Judgment [Doc. 1571] is therefore **GRANTED**.

c. Redressability

The last requirement that Plaintiffs must satisfy to establish Article III standing is redressability, meaning that CGG’s claimed injury must be “likely to be redressed by a favorable decision.” *See Jacobson*, 974 F.3d at 1245 (citing *Lujan*, 504 U.S. at 560–61). The State Defendants claim that CGG’s claims are not

⁶¹ The Court notes that the relevant state regulation focuses on pragmatic threats to the election process. Thus, “the types of events that may be considered emergencies are power outages, malfunctions causing a sufficient number of electronic ballot markers to be unavailable for use, or waiting times longer than 30 minutes.” Ga. Comp. R. & Regs. 183-1-12-.11(2)(d). Obviously, though, extremely long wait times and power outages or other serious malfunctions could have a serious impact on voters’ reasonable access to the polls.

⁶² The Plaintiffs still retain the right to seek a state mandamus remedy in Fulton County Superior Court pursuant to O.C.G.A. § 9-6-20 if the County refused to invoke its emergency authority to remedy a serious operational failure in the conduct of a specific election in the County at large or in any specific voting precinct, consistent with Ga. Comp. R. & Regs. 183-1-12-.11(2)(d).

redressable because the threat of election manipulation cannot be completely eliminated even under the organization’s preferred voting system — HMPBs. *See Weber v. Shelley*, 347 F.3d 1101, 1106 (9th Cir. 2003) (stating that “the possibility of electoral fraud can never be *completely* eliminated, no matter which type of ballot is used”) (emphasis original). They assert that issues such as equipment hacking, ballot security, and potential misconduct by local election officials can still affect other voting systems, and that CGG’s members can never be absolutely sure that their votes will be counted as cast, regardless of what election system the State puts in place.⁶³ But the Coalition Plaintiffs maintain that all of CGG’s injuries would be redressed if the State Defendants were enjoined from using the BMD system.

The Court recognizes that no election system is flawless. However, the inability to guarantee perfection does not prevent CGG from satisfying the redressability requirement because CGG is not claiming that its members have a right to a flawless election. *See Curling*, 334 F. Supp. 3d at 1318. Rather, as the Court previously explained, “Plaintiffs are seeking relief to address a particular voting system which they allege, as designed or as implemented by Defendants, burdens Plaintiffs’ capacity to cast votes that are actually properly counted and fails to produce a voter-verifiable auditable paper trail that is recognized as

⁶³ The Fulton County Defendants argue that Plaintiffs’ claims against them are not redressable because Fulton County cannot unilaterally adopt its own voting system without running afoul of state law mandating the use of BMDs. The Court need not reach the issue of whether Plaintiffs’ BMD-related claims against the Fulton County Defendants are redressable given its conclusion that those claims are not traceable to the Fulton County Defendants.

essential on a national level by election security experts.” (7/30/20 MTD Order, Doc. 751 at 44–45) (emphasis removed). In other words, “Plaintiffs are not asking for a system impervious to all flaws or glitches.” (*Id.* at 45) (quoting *Curling*, 334 F. Supp. 3d at 1319). Instead, “[t]hey are seeking to vindicate their right to effectively and reliably cast a verifiable vote reflective of their ballot choices.” (*Id.*)

Although the Court fully acknowledges that it “does not sit as a guarantor of a flawless election,” *Ga. Shift v. Gwinnett Cnty.* No. 1:19-cv-1135, 2020 WL 864938, at *6 (N.D. Ga. Feb. 12, 2020), the evidence presented by Plaintiffs at this juncture demonstrates it is feasible to provide meaningful relief to redress the challenged State conduct, practices, and associated harms at issue. While this relief may not extend to a new legislative Hand Marked Paper Ballot system that Plaintiffs seek as the gold standard, but which the legislature would have to enact, there are remedial measures that could be implemented without the Court invading the legislature’s sphere. Under the circumstances, the Court finds that the redressability requirement is satisfied.

Because Plaintiffs have adequately shown that CGG has suffered “(1) an injury in fact that (2) is fairly traceable to the challenged action of the defendant and (3) is likely to be redressed by a favorable decision,” *Jacobson*, 974 F.3d at 1245, the Court finds that CGG has provided sufficient evidence of Article III standing for purposes of summary judgment.

2. The Remaining Plaintiffs' Standing

The Court now considers the remaining Plaintiffs' standing to raise the broader BMD claims. Plaintiffs argue that due to the "One Plaintiff Rule," there is no need for the Court to address whether the other Plaintiffs have standing once it has confirmed CGG's standing. Under this rule, "the presence of one party with standing is sufficient to satisfy Article III's case-or-controversy requirement" and the Court need not determine whether other plaintiffs have standing before proceeding to the merits of a case. *See Rumsfeld v. Forum for Acad. & Institutional Rts., Inc.*, 547 U.S. 47, 52 n.2 (2006); *see also Fla. ex rel. Att'y Gen. v. U.S. Dep't of Health & Hum. Servs.*, 648 F.3d 1235, 1243 (11th Cir. 2011) (collecting cases) ("The law is abundantly clear that so long as at least one plaintiff has standing to raise each claim — as is the case here — we need not address whether the remaining plaintiffs have standing.") *aff'd in pertinent part, rev'd in part sub nom. Nat'l Fed'n of Indep. Bus. v. Sebelius*, 567 U.S. 519 (2012). Although the State Defendants acknowledge the foregoing authority, they argue that the Court should decline to apply the One Plaintiff Rule in this case.

The State Defendants first argue that the One Plaintiff Rule should only apply when each set of Plaintiffs is seeking identical relief. As support, they point to the Supreme Court's decision in *Town of Chester, New York v. Laroe Estates, Inc.*, 581 U.S. 433 (2017). There, the Supreme Court held that even when one plaintiff has standing, additional plaintiffs still must independently demonstrate that they have standing "in order to pursue relief that is different from that which

is sought by a party with standing.” *Id.* at 440. Stated another way, “[a]t least one plaintiff must have standing to seek each form of relief requested in the complaint,” and an additional plaintiff “must demonstrate Article III standing when it seeks additional relief beyond that which the plaintiff [with standing] requests.” *See id.* at 439.

The State Defendants thus argue that the Curling Plaintiffs⁶⁴ must independently demonstrate that they have Article III standing because they are seeking different relief than the Coalition Plaintiffs. They note that the two sets of Plaintiffs have filed separate Complaints using different phrasing for their requested relief, and that the Coalition Plaintiffs are seeking broader relief on certain discrete issues — including paper backups of the pollbooks and updates to the scanner settings. But as the Curling Plaintiffs note, each set of Plaintiffs are seeking the same core relief: to enjoin Defendants from using the BMD system as currently configured. It is of no consequence that the Coalition Plaintiffs are seeking relief beyond what the Curling Plaintiffs requested because the BMD-related relief sought by the Curling Plaintiffs is fully encompassed within the Coalition Plaintiffs’ requested relief. Indeed, the Curling Plaintiffs are not seeking “additional relief beyond that which the plaintiff [with standing] [here the CGG]

⁶⁴ The parties focus their One Plaintiff Rule arguments on whether the Curling Plaintiffs can proceed in the case based on the Coalition Plaintiffs’ organizational standing. However, the Court understands that only CGG may assert organizational standing and not the other individual Coalition Plaintiffs. Stated differently, it is “CGG” that has organizational standing and not “the Coalition Plaintiffs” more broadly. For that reason, the Court’s consideration of the One Plaintiff Rule has potential implications both for the Curling Plaintiffs and the individual Coalition Plaintiffs.

requests.” *Id.* In fact, it is the Coalition Plaintiffs — not the Curling Plaintiffs — that have requested some limited additional remedial measures beyond the core relief requested by both sets of Plaintiffs. As discussed later herein, these additional relief requests have not been granted. Thus, the One Plaintiff Rule properly applies here because the Curling Plaintiffs are seeking the identical core relief sought by the Coalition Plaintiffs and have not sought relief exceeding that core relief.

Defendants also emphasize that application of the One Plaintiff Rule is discretionary. *See Thiebaut v. Colo. Springs Utilities*, 455 F. App’x 795, 802 (10th Cir. 2011) (stating that “nothing in the cases addressing this principle suggests that a court *must* permit a plaintiff that *lacks* standing to remain in a case whenever it determines that a co-plaintiff has standing,” and adding that “courts retain discretion to analyze the standing of all plaintiffs in a case and to dismiss those plaintiffs that lack standing”) (emphasis original). They argue that there are multiple reasons why the Court should decline to exercise its discretion here.

First, the State Defendants argue that the One Plaintiff Rule was designed to promote judicial efficiency, *see id.* (stating that the One Plaintiff Rule “encourages judicial efficiency by permitting a court to proceed to the merits of a case involving multiple plaintiffs seeking identical relief when it is clear that at least one plaintiff has standing”), and that in some cases, rather than allowing all Plaintiffs to proceed in the case, it may better serve the interest of judicial efficiency to “par[e] down a case by eliminating plaintiffs who lack standing or otherwise fail to meet the governing jurisdictional requirements,” *see M.M.V. v. Garland*, 1 F.4th 1100, 1110

(D.C. Cir. 2021). In *M.M.V. v. Garland* — the case on which Defendants primarily rely — the court refused to apply the One Plaintiff Rule because doing so would have resulted in “more than 150 plaintiffs” proceeding with time-barred claims. *See id.* at 1111. Here, there are far fewer plaintiffs than in *M.M.V.* Indeed, there are only two sets of Plaintiffs, and just 8 Plaintiffs in total. The judicial efficiency concerns at issue in *M.M.V.* simply are not implicated here.

The State Defendants also argue that the One Plaintiff Rule should not apply when “an individual plaintiff’s standing has an impact on the case in some manner.” (State Defs.’ Reply Br., Doc. 1649 at 15–16.) In support, they cite *Federal Election Commission v. National Conservative Political Action Committee*, 470 U.S. 480 (1985). There, the FEC and a group of plaintiffs affiliated with the Democratic Party both sought declaratory relief to uphold the constitutionality of a provision of the Federal Election Campaign Act of 1971 (“FECA”). *Id.* at 482–84. The Supreme Court found that the FEC had standing based on a provision in FECA stating that the FEC “shall have exclusive jurisdiction with respect to the civil enforcement” of the Act. *Id.* at 485. But the Court declined to apply the One Plaintiff Rule to allow the other plaintiffs to piggyback on the FEC’s standing, because doing so “could seriously interfere with the agency’s exclusive jurisdiction to determine how and when to enforce the Act.” *See id.* at 485–86. In this case, there is no such analogous encroachment on a government agency’s exclusive jurisdiction.

Last, Defendants argue that the Court should decline to apply the One Plaintiff Rule because the two sets of Plaintiffs are represented by different attorneys who will be separately entitled to attorney's fees if they prevail in the case. However, Defendants cite no authority for the proposition that the potential for awarding multiple sets of attorney's fees is a legitimate basis for declining to apply the One Plaintiff Rule.

And to the contrary, Plaintiffs have identified at least one "major voting rights suit" — *Shaw v. Hunt*, 154 F.3d 161, 166 (4th Cir. 1998) — in which the court awarded attorney's fees to different sets of attorneys after earlier applying the One Plaintiff Rule. *See id.* at 167. In *Shaw*, the court awarded attorney's fees to a group of intervenor plaintiffs following a successful challenge to North Carolina's congressional districts, even though the intervenors lacked standing on their own. *See id.* at 163–64, 167. The court conferred the intervenor plaintiffs standing under the One Plaintiff Rule because there was at least one plaintiff with Article III standing and the intervenors "contributed significantly to the victory." *See id.* at 167.

Accordingly, even if some of the plaintiffs in this case were to lack independent standing, they may still be entitled to attorney's fees if they significantly contributed to the Plaintiffs' legally prevailing. Moreover, if Plaintiffs were to prevail on the merits of their claims *and* the work performed by the two sets of attorneys were truly duplicative, the Court could (and would) properly consider whether duplication of work by the attorneys warranted a reduction of

the fee award under 42 U.S.C. § 1988. However, this hypothetical has no bearing on the Court’s decision to apply the One Plaintiff Rule in the first place.

At bottom, the Court finds no basis for declining to apply the One Plaintiff Rule in these circumstances, and therefore concludes that the remaining Plaintiffs have standing to raise their asserted claims.

B. Are Plaintiffs’ DRE Claims Moot?

Having addressed standing, the Court is now faced with a different jurisdictional question: whether Plaintiffs’ DRE claims are moot. “Mootness is a jurisdictional question because the Court ‘is not empowered to decide moot questions or abstract propositions.’” *North Carolina v. Rice*, 404 U.S. 244, 246 (1971) (internal quotations omitted). “[A] case is moot when it no longer presents a live controversy with respect to which the court can give meaningful relief.” *Fla. Ass’n of Rehab. Facilities, Inc. v. State of Fla. Dep’t of Health & Rehab. Servs.*, 225 F.3d 1208, 1217 (11th Cir. 2000) (quoting *Ethredge v. Hail*, 996 F.2d 1173, 1175 (11th Cir. 1993)).

The State Defendants argue that Plaintiffs’ DRE claims are moot because the State has completely transitioned from the DRE system to the BMD system, as authorized by HB 316, and because DREs have not been used in any Georgia elections since the Court entered its PI Order in 2019.⁶⁵ State Defendants also point out that the Court has stated that it “does not intend to grant any further relief

⁶⁵ They add that the current legislative scheme would prohibit the State from changing back to the DRE system.

relating to the use of the old DRE voting machines.” (State Defs.’ MSJ, Doc. 1567-1 at 20) (citing 7/30/20 MTD Order, Doc. 751 at 20). They also point to the Curling Plaintiffs’ lead counsel David Cross’s representation that all parties agree that the Counts pertaining to the DRE claims “are moot.” (*Id.* at 18) (quoting 11/19/21 Hr’g Tr., Doc. 1234 p. 73.)

On the other side of the dispute, Plaintiffs either agree or do not dispute that any challenge to the State’s use of DREs is moot. However, both groups of Plaintiffs argue that the DRE claims are *not totally* moot to the extent that they challenge particular components of the DRE system that were carried over to the current BMD system: namely, the voter registration database. (Curling Pls.’ Opp’n, Doc. 1636 at 35.)

On review, the Court finds that claims challenging the DRE voting machines themselves — specifically Counts I and II of the Coalition Plaintiffs’ Third Amended Complaint and Counts I and II of the Curling Plaintiffs Third Amended Complaint — are moot. After the enactment of HB 316, the State fully transitioned to a new voting system. This “comprehensive electoral reform[]” prevents the State Defendants from returning to the old system even if it wanted to, rendering any challenge to the old system moot. *United States v. Georgia*, 778 F.3d 1202, 1205 (11th Cir. 2015).

While any challenge to the use of the DRE machines no longer presents a live controversy, Plaintiffs may still challenge and present evidence on elements of the DRE system that carried over to the BMD system, specifically evidence

involving the voter registration database as a component of the existing voting system and the policies and practices regarding matters such as updating of software patches. The Court considers such evidence as reasonably within the parameters of Plaintiffs' substantive BMD-related claims. With the above caveat and condition, the Court **GRANTS** summary judgment in favor of the State Defendants on Counts I and II of the both the Curling and Coalition Plaintiffs' Third Amended Complaints, i.e., the DRE claims.

C. Merits of Plaintiffs' Fundamental Right to Vote and Equal Protection Claims

Having determined that the Plaintiffs have standing, the Court next assesses Plaintiffs' constitutional claims on the merits.

1. Plaintiffs' Constitutional Claims Challenging the BMD System

The claims remaining in this case are: the Curling Plaintiffs' Counts III (violation of the fundamental right to vote under the Due Process Clause of the Fourteenth Amendment) and IV (violation of the Equal Protection Clause of the Fourteenth Amendment), and the Coalition Plaintiffs' Counts I (violation of the fundamental right to vote under the First and Fourteenth Amendments) and II (violation of the Equal Protection Clause of the Fourteenth Amendment).

In this Circuit, courts analyze First and Fourteenth Amendment claims that challenge election practices under the balancing test outlined by the Supreme Court in *Anderson v. Celebrezze*, 460 U.S. 780 (1983) and *Burdick v. Takushi*, 504 U.S. 428 (1992). See *Democratic Exec. Comm. of Fla. v. Lee*, 915 F.3d 1312, 1318

(11th Cir. 2019). Most of the parties agree that this test should apply to each of Plaintiffs’ constitutional claims.⁶⁶ The Court is not convinced that an alternative test should apply to any of the First and Fourteenth Amendment claims Plaintiffs raise here, and will therefore analyze all of these claims together under the *Anderson-Burdick* test.

This test requires the Court to “weigh the ‘character and magnitude’ of the burden that the State’s rule imposes” on Plaintiffs’ voting rights “against the interests that the State contends justify that burden, and consider the extent to which the State’s concerns make the burden necessary.” *Timmons v. Twin Cities Area New Party*, 520 U.S. 351, 358 (1997) (citing *Burdick*, 504 U.S. at 434). Ultimately, “the level of the scrutiny to which election laws are subject varies with the burden they impose on constitutionally protected rights.” *Stein v. Alabama Sec’y of State*, 774 F.3d 689, 694 (11th Cir. 2014).

Laws that severely burden the right to vote “must be narrowly drawn to serve a compelling state interest.” *Lee*, 915 F.3d at 1318 (citing *Burdick*, 504 U.S. at 434). But “reasonable, nondiscriminatory restrictions that impose a minimal burden may be warranted by the State’s important regulatory interests.” *Billups*, 554 F.3d at 1352 (cleaned up). “And even when a law imposes only a slight burden on the right to vote, relevant and legitimate interests of sufficient weight still must justify that burden.” *Lee*, 915 F.3d at 1318–19 (citing *Billups*, 554 F.3d at 1352).

⁶⁶ The Fulton County Defendants are the only party who argued that a traditional equal protection analysis should apply to Plaintiffs’ equal protection claims instead of the *Anderson-Burdick* test. As no other party asserts this argument, the Court does not address this contention.

a. *Anderson-Burdick* Step One

Consistent with the above authority, the Court first considers “the character and magnitude of the burden” imposed by the allegedly unconstitutional conduct. *See Timmons*, 520 U.S. at 358 (citation omitted). Here, the Court understands the claimed constitutional burden to be the risk of harm that the current election system’s security vulnerabilities and operational issues imposes on Plaintiffs’ right to cast an effective, accurately counted vote. The State Defendants argue that the BMD system imposes no constitutional burden. But Plaintiffs contend that the burdens are severe, or at the very least, that there is a question of fact as to the magnitude of the burden.

In the 2020 PI Order, the Court stated that, based on the then-proffered evidence, it viewed “the burden and the threatened deprivation as significant” under step one of the *Anderson-Burdick* test. (10/11/20 PI Order, Doc. 964 at 79.) The Court remarked that the “substantial risks and long-run threats posed by Georgia’s BMD system” were “evident,” and included “serious system security vulnerability and operational issues that may place Plaintiffs and other voters at risk of deprivation of their fundamental right to cast an effective vote that is accurately counted.” (*See id.* at 89, 143.) Based on the presented evidence, the Court ultimately concluded that the Plaintiffs “put on a strong case indicating they may prevail on the merits at some future juncture.” (*Id.* at 144).

Since then, the evidentiary record in this case has grown. The 2021 Halderman Report, CISA’s 2022 security advisory corroborating the Halderman

Report, and the revelations regarding the 2021 Coffee County voting system breach are among the important new evidence that arguably further support the substantial risks posed by Georgia's BMD voting system. As the Court must view the facts in the light most favorable to Plaintiffs on summary judgment, their proffered evidence in support of their allegations — that the State's election system as currently configured presents an actual or imminent threat to Plaintiffs' constitutional right to have their votes counted as cast — is sufficient at this stage. Ultimately, the Court concludes that for the purpose of summary judgment, there is a sufficient question of material fact regarding the magnitude of the burden imposed by Georgia's BMD voting system to warrant denial of the State Defendants' Motion for Summary Judgment.

Despite the strength of the record Plaintiffs' put forward, the State Defendants argue that there are a variety of reasons why the Court should decline to permit this case to proceed to trial on the merits. Upon review, none are sufficiently persuasive as to justify granting summary judgment.

First, the State Defendants argue that Plaintiffs cannot succeed on their due process claims without affirmative state action. Specifically, they argue that failure to prevent hacking or to mitigate cybersecurity vulnerabilities constitutes only *inaction* by the State, which does not give rise to a colorable due process claim. The Eleventh Circuit previously rejected this argument in the context of Plaintiffs' DRE claims. *See Curling v. Sec'y of State of Ga.*, 761 F. App'x 927, 933 (11th Cir. 2019) (explaining that the Plaintiffs challenge "both the State Defendants' affirmative

conduct and inaction,” and also noting that settled precedent allows for suits based on the argument that “state officials’ inaction allegedly harms constitutional rights”). The Court finds no basis to reach a different conclusion with respect to Plaintiffs’ BMD claims.

Second, the State Defendants argue that the Court should decline to hear the case because it presents a non-justiciable political question. At least in the context of the pollbook claim, the Eleventh Circuit has also already rejected that argument. *See Curling*, 50 F.4th at 1121 n.3 (finding that the Coalition Plaintiffs’ claims do not “present a political question beyond the Court’s reach”).

In the current motions, the State Defendants argue that the burdens at issue in Plaintiffs’ broader challenge to the BMD system present non-justiciable questions because they are not the sort of burdens that would permit the Court to engage in *Anderson-Burdick* balancing. In support, the State Defendants rely on a portion of the Eleventh Circuit’s decision in *Jacobson*.

There — in considering a challenge to a Florida statute governing the order in which candidates’ names appeared on the ballot — the Eleventh Circuit found that it was “impossible to identify a burden on voting rights imposed by the ballot statute” that was “susceptible to the balancing test of *Anderson* and *Burdick*.” *Jacobson*, 974 F.3d at 1261. The court explained that the statute was “unlike any law that [the Eleventh Circuit] or the Supreme Court has ever evaluated under *Anderson* and *Burdick*,” in that it did not, among other things, “make it more difficult for individuals to vote or to choose the candidate of their choice,” “limit

any political party's or candidate's access to the ballot," or "create the risk that some votes will go uncounted or be improperly counted." *See id.* at 1261–62 (internal citations omitted). Instead, the challenged statute merely "determine[d] the order in which candidates appear in each office block on the ballot." *Id.* at 1262.

But here, the burden Plaintiffs identify is one that *Jacobson* expressly *recognized* as subject to balancing under *Anderson* and *Burdick* — namely, "the risk that some votes will go uncounted or be improperly counted." *See id.* at 1262. The State Defendants' reliance on *Jacobson* is therefore misplaced.

Third, the State Defendants argue that Plaintiffs' claims must fail because electronic voting systems do not impose a "severe burden" simply by virtue of being electronic. (State Defs.' Reply, Doc. 1650 at 18). This argument is also unavailing.

It is true that electronic voting systems are not *per se* unconstitutional. *See Banfield v. Cortes*, 110 A.3d 155, 178 (Pa. 2015) (rejecting constitutional challenge to Secretary of State's decision to certify electronic voting system). But Plaintiffs are not challenging the BMD system merely because it is electronic — they are challenging the current *configuration and implementation* of Georgia's BMD voting system. (*See* 7/30/20 MTD Order, Doc 751 at 40) ("Plaintiffs challenge the State Defendants' implementation of a barcode-based [BMD] system with known and demonstrated vulnerabilities contrary to the recommendations of voting system experts that is incapable of being properly audited.") Indeed, since the onset of this case, Plaintiffs have presented specific evidence of data exposure events and unaddressed system vulnerabilities in support of their claims.

Fourth, the State Defendants note that Plaintiffs’ policy preference for a paper ballot system is an issue for the legislature. The Court agrees that, to the extent Plaintiffs are seeking to have the Court order the State to switch to a HMPB system, the Court lacks the authority to grant that specific relief. In fact, the Court has reiterated this limitation since the earliest stages of this case. It is well established that even if Plaintiffs prevail on their substantive claims, the Court cannot require the State to make a statewide switch to HMPBs without encroaching upon the State legislature’s power. *See Burdick*, 504 U.S. at 433–34; *Wood*, 501 F. Supp. 3d at 1327–28.

But as the Eleventh Circuit previously recognized, “Plaintiffs do not seek a court order directing the precise way in which Georgia should conduct voting. Instead, Plaintiffs seek only injunctive and declaratory relief against a system that they decry as unconstitutionally insecure.” *Curling*, 761 F. App’x at 934. Thus, if the Plaintiffs succeed in challenging the State’s use of the BMD system as it is currently configured — e.g., without implementing a software patch to address the vulnerabilities identified by Dr. Halderman and corroborated by CISA, utilizing QR codes that arguably enhance the risk of errors in the tabulation of Plaintiffs’ votes, and lacking sufficient audits to ensure that issues would be caught — there may be sufficient grounds for the Court to enter injunctive relief directing the State

Defendants to implement tailored remedial measures, given sufficient proof at trial.⁶⁷

Fifth, the State Defendants argue that to the extent the BMD system imposes a constitutional burden, Plaintiffs could avoid that burden simply by voting absentee. For this argument, the State Defendants rely on the Eleventh Circuit’s decision in *New Georgia Project v. Raffensperger*, 976 F.3d 1278 (11th Cir. 2020). There, the Eleventh Circuit stayed a district court order enjoining the State from enforcing Georgia’s “decades-old” absentee ballot deadline during the 2020 general election due to the effects of the COVID-19 pandemic. *See id.* at 1280, 1284. The district court reasoned that the State’s refusal to extend the deadline constituted a “severe” burden on voters because “a potentially substantial backlog” of requested absentee ballots could result in some voters missing the deadline and having their ballots rejected. *See id.* at 1281 (citation omitted).

⁶⁷ The Court recognizes that a switch to HMPBs is Plaintiffs’ preferred remedy in this case. However, the Curling Plaintiffs have also made it clear that a wholesale change to paper ballots is not the only possible remedy. For example, in their Statement of Material Facts, Plaintiffs stated that simply eliminating the QR code component of the BMD system “would somewhat mitigate” their injuries. (Pls.’ Statement of Additional Facts, Doc. 1637 ¶ 159.)

Lead counsel for the Curling Plaintiffs, David Cross, made a similar point at oral argument. (*See* 5/2/23 Hr’g Tr., Doc. 1668 at ECF 17.) (“Lastly, Your Honor, while Mr. Tyson is right that eliminating a QR code will not give us the full scope of the relief we’re asking for, it is certainly a critical component of the relief we’re asking for. So if that is all we got — certainly we hope it is not. We think we’re entitled to more — but that is part of the relief that we’re asking for. And I wanted to make that clear.”).

And at least one Plaintiff has suggested that her claims might potentially be addressed if the State Defendants performed more robust audits. (*See* Jan. 19, 2022 Dep. of Donna Curling, Doc. 1570-1 at 71) (“Q. If the Court were to order — and I understand it’s a hypothetical; but if the Court were to say we’re going to keep the BMDs as they are but order risk-limiting audits as even Dr. Stark suggests, would your concerns about elections be resolved? . . . THE WITNESS: I would have to think about it more deeply, but just my first impression is yes.”).

In granting the defendants’ motion to stay the district court’s injunction, the Eleventh Circuit explained that under step one of the *Anderson-Burdick* test, “it is just not enough to conclude that if some ballots are likely to be rejected because of a [state election] rule, ‘the burden on many voters will be severe.’” *Id.* (citation omitted). It also noted that the absentee ballot deadline was a nondiscriminatory election rule that — like rules governing in-person and drop-box voting — imposed a “reasonable burden” on voters to “exert some effort to ensure that their ballots are submitted on time.” *See id.* at 1282, 1284. And to the extent that COVID increased the demand for absentee ballots and risked some voters receiving their mail-in ballots at too late a date, the Eleventh Circuit emphasized that Georgia “provided numerous avenues to mitigate chances that voters will be unable to cast their ballots,” including by providing the opportunity to engage in early voting, in-person voting, or by submitting their ballot by drop box. *See id.* at 1281–82. Thus, the court held that because the challenged deadline “imposes only a reasonable burden even on absentee voters who receive their ballots later than usual, the State’s interests easily survive the *Anderson-Burdick* framework.” *Id.* at 1282.

Here, the State Defendants distort the Eleventh Circuit’s holding in *New Georgia Project* to argue that “the widespread availability of absentee voting to all voters including Curling Plaintiffs . . . dooms their claim” challenging the use of Georgia’s BMD systems. (*See* State Defs.’ Reply, Doc. 1649 at 26). They assert that “if the ability to vote in-person remove[d] any burden for absentee voting” in *New Georgia Project*, then “surely the ability to vote absentee removes any burden for

in-person voting” in this case. (State Defs.’ Reply, Doc. 1649 at 26.) The Court sees several problems with this argument.

To start, the Eleventh Circuit did not hold that, for the purposes of the *Anderson-Burdick* analysis, the availability of alternative voting methods “removes any burden” imposed on a certain voting method. Such a holding has no basis in established case law,⁶⁸ because courts — including the Eleventh Circuit in *New Georgia Project* — routinely find that burdens have been imposed on one method of voting despite the existence of other voting methods.⁶⁹ *See, e.g., New Georgia Project*, 976 F.3d at 1282 (recognizing that the challenged absentee ballot deadline imposed “a reasonable burden” on absentee voters despite discussing at length the other voting options available).

Instead, the Eleventh Circuit’s holding in *New Georgia Project* is more modest. It simply states that Georgia’s unwillingness to alter its decades-old absentee ballot deadline to accommodate potential COVID exigencies did not transform an otherwise “reasonable, nondiscriminatory” voting rule into a “severe” burden on absentee voters, particularly where alternative voting methods could help voters submit a timely vote if they received their absentee ballot too late. *See id.* at 1284. The court thus concluded that the State’s administrative interests

⁶⁸ And troublingly, such a rule would seem to have the perverse effect of enabling state actors to engage in potentially antidemocratic gamesmanship with election regulations to favor certain voting methods over others.

⁶⁹ After all, a constitutional burden is still susceptible to balancing under the *Anderson-Burdick* test even if it is not “severe.” *See Billups*, 554 F.3d at 1352 (“However slight [the] burden may appear, ... it must be justified by relevant and legitimate state interests sufficiently weighty to justify the limitation.” (alterations in original) (quoting *Crawford v. Marion Cnty. Election Bd.*, 553 U.S. 181, 191 (2008))).

“easily” justified the “reasonable burden” the deadline imposed on absentee voters. *See id.* at 1282.

Here, Plaintiffs claim that Georgia’s current BMD voting system imposes a severe constitutional burden on their right to have their votes accurately counted as cast. Viewing all facts and inferences in Plaintiffs’ favor, the Court concludes that for the purpose of summary judgment, there is a sufficient question of fact as to the burden imposed by Georgia’s BMD voting system for this case to proceed past summary judgment.

b. *Anderson-Burdick* Step Two

Next, the Court considers the State’s justifications for the burdens imposed by the BMD system and “the extent to which the State’s concerns make the burden necessary.” *See Timmons*, 520 U.S. at 358. Here, it may well be that the burden is only a “slight” one. If that is the case, “the State need not establish a compelling interest to tip the constitutional scales in its direction.” *Burdick*, 504 U.S. at 439, But no matter how slight the burden may be, “relevant and legitimate interests of sufficient weight” must still justify it. *Lee*, 915 F.3d at 1318–19.

Construing all facts and inferences in Plaintiffs’ favor, the Court concludes that even if the BMD voting system only imposes a slight burden on Plaintiffs’ voting rights, there remains a genuine dispute of material fact as to whether the State’s regulatory interests sufficiently justify the imposition of those burdens. Although at this juncture the Court is not in a position to consider the weight of the State Defendants’ proffered justifications, it notes that based on the formidable

record Plaintiffs have assembled, it is not clear that a generically invoked regulatory interest, such as a general interest “in conducting orderly elections,” will be sufficient to justify the decision to maintain the current configuration of Georgia’s BMD voting system without adopting any of remedial measures identified by CISA, Dr. Halderman, Fortalice, or other experts.

D. Remaining Components of Coalition Plaintiffs’ Claims

Having addressed the Plaintiffs’ primary constitutional challenges to the BMD system, the Court now turns to the Coalition Plaintiffs’ remaining theories of constitutional violations. In conjunction with their broader challenges to the BMD system, the Coalition Plaintiffs separately challenge other aspects of the BMD system related to (1) ballot secrecy, (2) scanner settings used to count absentee ballots, and (3) the voter registration database information provided by the State to the counties by way of the pollbook and PollPads. Before diving into the merits, the Court provides a brief procedural history of prior arguments and rulings on these issues.

1. Procedural History

The Court first addressed these three issues upon review of the Coalition Plaintiffs’ 2020 PI motion. In their 2020 motion, as to relief, the Coalition Plaintiffs did not seek specific relief measures related to their ballot secrecy arguments. As to scanner settings, the Coalition sought to require Defendants to adjust the settings on Dominion’s optical scanners to provide more complete and accurate capture of hand-made voting marks on absentee ballots so that these

ballots could be properly reviewed and counted where the markings were decipherable and manifested voter intent as to the ballot selections made. As to the paper backup of pollbook information issue, the Coalition Plaintiffs sought to require the Secretary of State's Office to provide county election superintendents with more up-to-date paper backups of the pollbook information to facilitate efficient and accurate processing of voters at the polls and remedy the long lines that had characterized early voting and use of the BMDs and pollbooks. (9/28/20 Paper Backup PI Order, Doc. 918 at 3; 10/11/20 PI Order, Doc. 964 at 3.)

Upon review of the Coalition Plaintiffs' 2020 PI motion, the Court first concluded that the Coalition Plaintiffs had not established a likelihood of success on the merits as to their ballot secrecy constitutional arguments.

Second, as to the Coalition Plaintiffs' scanner settings argument, the Court recognized serious problems with the scanner settings used by Defendants to capture vote selection markings on paper ballots, given the direct impact of the scanner settings on whether paper ballot voting selections could be properly read, and in light of Georgia law's statutory requirement that votes "shall be counted" where "the elector has marked [her] ballot in such a manner that [she] has indicated clearly and without question the candidate for whom [she] desires to cast [her] vote." *See* O.C.G.A. § 21-2-438(c). The Court therefore concluded that the Coalition Plaintiffs were entitled to injunctive relief on this issue. (10/11/20 PI Order, Doc. 964 at 140–41.) The Court directed the Coalition Plaintiffs to submit their own proposed injunctive relief measures as to appropriate scanner settings

for the Court’s consideration and deferred ruling on the specifics of the injunctive relief in the interim. (*Id.* at 141–42.)

Finally, as to the third issue, the Court — by separate Order — recognized evidence of electronic PollPad malfunctioning and inadequate paper backups of the voter data required for processing voters expeditiously and accurately at the polls. The Court issued an Order directing the Secretary of State to transmit paper backups of the pollbooks to county election supervisors at the close of in-person early voting to ensure that the paper backups would include up-to-date information in the event of electronic PollPad failures. (9/28/20 Paper Backup PI Order, Doc. 918 at 63–66.)

The State Defendants subsequently appealed both the Paper Backup Order and the Scanner Settings Order (and did so before the Court could order any relief related to the scanner settings). On appeal, the Eleventh Circuit vacated the district court’s Paper Backup Order and declined to address this Court’s ruling on the scanner settings claim, as the Court had not ordered a specific remedy. *See Curling v. Raffensperger*, 50 F. 4th 1114, 1125–1126 (11th Cir. 2022).⁷⁰

At summary judgment, the Coalition Plaintiffs continue to seek relief on these issues. As such, the Court now reviews these issues anew.

⁷⁰ The Coalition Plaintiffs did not file a fresh request for relief on the scanner settings issue after the Eleventh Circuit’s ruling. While the Coalition Plaintiffs might conceivably have been waiting for the Court to schedule a hearing on this issue, the Coalition Plaintiffs and their counsel have never been shy about requesting hearings.

2. Ballot Secrecy

In their First Supplemental Complaint (Doc. 628), the Coalition Plaintiffs alleged, as a part of Counts I and II, that the BMD system burdens their right to vote and deprives them of equal protection because it denies them the right to vote on a secret ballot. (*See e.g., id.* ¶¶ 127, 129, 203, 223, 231.)⁷¹ In short, the Coalition Plaintiffs contend that the BMD system deprives them of a secret ballot because (1) the large, brightly-lit screens are visible to other voters and poll workers, and (2) the ICP scanners provide certain records that, when compared to other information (scanner voter counts, polling place video, etc.), make it possible to match ballot images to voters. (*See* First Supp. Compl., Doc. 628 ¶¶ 121–129, 194, 223; Coalition Pls.’ Opp’n, Doc. 1624 at 72–73.) The Coalition Plaintiffs further alleged that the State Defendants’ failure to ensure a secret ballot exposes them to the “potential for identification, retaliation, and accountability based upon their elector choices.” (*Id.* ¶ 127.)

The Court previously addressed the Coalition Plaintiffs’ arguments on ballot secrecy in its October 2020 Preliminary Injunction Order. (Doc. 964 at 89-93.)

⁷¹ The Coalition Plaintiffs also alleged that the BMD system deprived them of a secret ballot in violation of the Georgia Constitution and Georgia statutory law in Count III, their procedural due process claim (*id.* ¶ 240). In July of 2020, the Court dismissed without prejudice Count III because the Coalition Plaintiffs did not allege “that the State Defendants have failed to provide adequate procedures to remedy the alleged harms.” (7/30/20 Order, Doc. 751 at 49-51.) The Court further noted that the Coalition Plaintiffs could not rely on the failure of the State Defendants to provide due process where adequate state remedies were available in the state courts, specifically via a writ of mandamus to address Plaintiffs’ alleged harm under Georgia law. (*Id.* at 50 n.28.) Consequently, at this juncture, to the extent Plaintiffs assert that the lack of a secret ballot violates the Georgia Constitution or Georgia statutes, such an argument is outside the scope of this case, having been addressed and dismissed without prejudice by the Court’s prior Order.

There, the Court denied any form of relief related to ballot secrecy because the Coalition Plaintiffs failed to establish a likelihood of success on the merits on this issue. (*Id.*) In particular, the Court noted that, although the Coalition Plaintiffs presented some evidence of voter discomfort, they presented (1) no evidence from any voter claiming that the publication of their vote selections subjected them to threats, harassments, or reprisals, and (2) no evidence of “actual infringement of voter anonymity as a result of the use of digitally recorded scanner timestamp records.” (*Id.*)

Now, in renewing this argument at summary judgment, the Coalition Plaintiffs once again rely on affidavits from voters who have experienced discomfort as a result of large, bright screens and also the possibility of matching ballots to voters. (*See, e.g.*, Jan. 31, 2023 Decl. of Virginia Forney ¶¶ 12–19 (noting concerns related to public visibility of the touchscreens as well as the “permanent traceable record that I’ve recently learned is available because of the non-randomized recording of votes in the scanner”); Feb. 7, 2023 Decl. of Jeanne Dufort, Doc. 1593 ¶¶ 16–21 (outlining “personal concerns with casting my vote without reasonable ballot secrecy” especially “in a small county like Morgan [County],” both as to viewability of touchscreens and ability to match a ballot image with a voter)). The Coalition Plaintiffs have also introduced evidence that Dr. Halderman more recently discovered a vulnerability in Dominion’s scanners that could allow someone, *theoretically*, to “‘unshuffle’ ballot-level data . . . such as ballot images or cast vote records, and learn the order in which they were scanned,”

and use that information to connect cast vote records to voters. (*See* Oct. 11, 2022 Letter from Halderman to Blake Evans, Doc. 1590-1.)

Even accepting this evidence as true (as required at summary judgment), the Coalition Plaintiffs still present no evidence to suggest that poll workers or members of the public will attempt (or have attempted) to either observe their voting selections or go through the multi-step process of associating their voting selections with specific ballot images or cast vote records. As such, the Coalition Plaintiffs fail to present any evidence that these potential concerns surrounding ballot secrecy have produced any chilling effect on their ability to exercise their rights to vote.⁷² In light of this dearth of evidence that the Coalition Plaintiffs’ ballot secrecy discomforts “make it more difficult for [the Coalition Plaintiffs or their members] to vote . . . or to choose the candidate of their choice,” they cannot establish a legally viable burden. *Jacobson*, 974 F.3d at 1261.⁷³ Absent evidence to

⁷² As previously discussed, Plaintiffs have presented sufficient evidence to suggest United States and Georgia elections are targets for hacking by malicious actors — at least for purposes of summary judgment. But the Coalition Plaintiffs have presented no evidence to suggest that anyone — hackers, malicious poll workers, or even neighborhood busybodies — actually seek to discover how they or their members personally voted, or that they or their members have been in any way prevented from voting their conscience. Thus, unlike their broader challenge to the BMD system on the ground that it creates a material risk that their votes “will go uncounted or be improperly counted,” the Coalition Plaintiffs’ separate ballot secrecy challenges have not resulted in any evidence of a burden on the right to vote “that is susceptible to the balancing test of *Anderson and Burdick*.” *Jacobson*, 974 F.3d at 1261.

⁷³ The Court, however, recognizes the reality that the large, bright screens can be seen by other voters and poll workers. (Feb. 7, 2023 Decl. of Aileen Nakamura, Doc. 1597 ¶ 17) (“Based on my personal observations, in every polling place I have observed, it is almost always possible to see how voters are voting from certain angles or when one is walking past a voter, no matter the equipment configurations attempted.”). The Court also recognizes that possible solutions to this issue exist — such as the State’s purchase and provision of privacy screens. However, in light of the governing legal authority, such a fix falls within the realm of the State’s administrative and regulatory authority.

support a legally viable burden on the Coalition Plaintiffs' right to vote, this ballot secrecy component of the Coalition Plaintiffs' claims cannot proceed to trial.⁷⁴

3. Scanner Settings

Next, the Court addresses the Coalition Plaintiffs' request for relief as to ICC scanner settings used for absentee hand ballots completed by the voter's hand markings. For context: without proper adjustment of scanner settings, the optical scanners show more ballot "blanks" in each race's voting "bubble" to be filled out with the voter's candidate selection. While the ballot instructions do advise voters to fill in the ballot bubbles, Georgia law explicitly provides that voters who have marked their choices with an X or check mark (✓) must be reviewed by the local election office adjudication board, and if clearly reflecting voter intent, be counted in the vote tally. *See* O.C.G.A. §§ 21-2-438(b)&(c)⁷⁵; Ga. Comp. R. & Regs. 183-1-15-.02(2)(2).

⁷⁴ As noted above, however, the Coalition Plaintiffs' claims and arguments that the lack of a secret ballot violates the Georgia Constitution or Georgia law has not been adjudicated in this case, and they therefore may further pursue those arguments in state court.

⁷⁵ Sections (b) and (c) of O.C.G.A. § 21-2-438 provide as follows:

(b) At elections, any ballot marked by any other mark than a cross (X) or check (✓) mark in the spaces provided for that purpose shall be void and not counted; provided, however, that no vote recorded thereon shall be declared void because a cross (X) or check (✓) mark thereon is irregular in form. A cross (X) or check (✓) mark in the square opposite the names of the nominees of a political party or body for the offices of President and Vice President shall be counted as a vote for every candidate of that party or body for the offices of presidential elector.

(c) Notwithstanding any other provisions of this chapter to the contrary and in accordance with the rules and regulations of the State Election Board promulgated pursuant to paragraph (7) of Code Section 21-2-31, if the elector has marked his or her ballot in such a manner that he or she has indicated clearly and without question the candidate for whom he or she desires to cast his or her vote, his or her ballot shall be counted and such candidate shall receive his or her vote, notwithstanding the fact that the elector in indicating his or her choice may have marked his or her ballot in a manner other than as prescribed by this chapter.

In the latter part of the 2020 election cycle, after complaints raised by CGG and its members as well as national news articles about this issue, the State Board of Elections approved a modification in the scanner settings that partially — but not fully — addressed this important problem. (*See* 10/11/2020 Order, Doc. 964 at 122–23.) This resulted in a larger number of hand ballots being reviewed on the local election board level to assess whether the voter had clearly indicated each of his or her intended ballot selections. However, in the Coalition Plaintiffs’ view, there remained additional software and technology issues that needed to be addressed to ensure accurate and full reporting of the scanned hand ballot votes. (10/11/2020 PI Order, Doc. 964 at 93–142.)

The Coalition Plaintiffs contended in the 2020 PI proceedings, and now do again, that the change in the scanner settings approved by the State Board of Elections did not address the full scope of the hand marked ballots votes still being skipped and not counted by the scanners. (Coalition Pls.’ Resp., Doc. 1624 at 74–75.) At the PI hearing, the Coalition Plaintiffs’ expert on scanner technology, Harri Hursti, testified that further adjustments in the scanner software were both technically feasible and necessary to improve the quality of the scanning process and images so as to make hand marks more clearly visible for review. These technical adjustments would allow proper review and counting of visible additional ballot marks as cognizable votes. (*See generally* 10/11/2020 PI Order, Doc. 964 at 99–104.) Mr. Hursti testified at the 2020 preliminary injunction hearing that the ICC central count scanner “can be configured to capture higher quality and more

information retaining images” and also is capable of producing images of a significant higher order of magnitude than it currently produces based on Dominion’s programming. (*Id.* at 126, 133–34.) As Hursti explained, “the way the scanner is used in this environment is like driving your sports car locked on the first gear.” (*Id.* at 134.) Further, Hursti explained that the central count scanner is recording a lower quality image than it is capable of because, “as part of the configuration, that scanner is instructed to produce low quality images with a reduced amount of information.” (*Id.*)⁷⁶ Hursti proceeded to make specific remedial recommendations.

As evidenced by its 2020 PI Order, the Court is troubled by the Defendants having not proceeded to implement additional adjustments in their scanner software to maximize the State’s capacity to ensure that all hand ballot votes are properly and fully counted to the extent reasonably feasible. Indeed, the prospect of uncounted legitimate votes resulting from use of default scanner settings that are not sufficiently refined to properly determine voter intent on some unknown number of hand-marked absentee ballots where there are clear markings (but the ballot bubbles are not fully colored in) is disturbing. But, upon review of the current record, the Court concludes that the Coalition Plaintiffs have not provided sufficient evidence that the State’s current scanner settings for counting absentee

⁷⁶ Coalition member Jeannie Dufort also testified at the 2020 hearing of her experience in feeding a series of test hand ballots into a scanner in four possible ways and receiving different information each time identifying different messages as to which hand votes were ambiguous. (10/11/2020 PI Order, Doc. 964 at 104–105.)

ballots rises to the level of a serious burden on their fundamental voting rights sufficient to overcome the State’s regulatory interest in administering the election using existing settings.⁷⁷ *Curling v. Raffensperger*, 50 F.4th at 1122–25 (“[I]f federal courts were to flyspeck every election rule . . . our enforcement practices would bar States from carrying out their constitutional responsibility to prescribe election rules.”)

As the evidence demonstrates, this is a complex issue requiring further analysis for assessing the best technical adjustments needed on the road ahead. For that reason, among others, the Court concludes that the scanner settings issue is best addressed by the State Election Board or through the Georgia courts based upon the clear statutory mandates, outlined above, that seek to ensure that hand ballots are fully reviewed for markings indicating “voter intent” and that such votes be included in vote tallies where so warranted. While the Court recognizes why the Coalition sought relief in connection with the scanners pursuant to their substantive constitutional claims in this case, this portion of their relief claim rests in large part on state law guarantees and technical issues that require follow-up.

⁷⁷ As the Court noted in its prior Order (Doc. 964), the State Election Board, in September of 2020, approved a regulation instructing that the ICC scanners be set such that “[d]etection of 20% or more fill-in of the target area surrounded by the oval shall be considered a vote for the selection.” (*Id.* at 122–23.) This was a lower percentage setting than the default setting of 35% that had previously been used. (*Id.* at 101.) The burden imposed by the previous 35% setting might have constituted a serious burden given the data presented to the State Board of Elections and later reviewed by this Court. While the Court does not question Mr. Hursti’s expert testimony regarding the additional software and technical modifications that could heighten the scanners’ precision, the Court has insufficient information before it at this time to assess the scope of the impact of the additional software modifications Mr. Hursti recommended.

Accordingly, this Court cannot grant relief on this issue as part of the proceedings in this case.

4. Pollbooks/PollPads

Finally, in challenging the BMD system and all its relevant components, the Coalition Plaintiffs also raise issues related the security and reliability of Georgia's voter registration database, electronic pollbooks, and PollPads.⁷⁸

As refresher background information, on Election Day, the State's primary way of checking in voters for in-person voting "is with computer tablets containing lists of eligible voters in each precinct. These [tablets] are also known as 'PollPads.'" *Curling v. Raffensperger*, 50 F.4th at 1118. To create the PollPad check-in lists, the State uses its electronic voter registration database. *Id.* Prior to Election Day, as early voting proceeds, the voter registration database and the PollPads are "updated to reflect whether voters have requested absentee ballots, voted absentee, or voted early." *Id.* In the event of errors or malfunctions with the PollPads, state law requires each precinct to have a paper backup list. *See* Ga. Comp. R. & Regs. 183-1-12-.19(1). Each of Georgia's 159 counties may order its paper backup list during a period ending the week before the election. *Id.* The counties then distribute the sub-lists to their precincts. *Id.* But, because the paper

⁷⁸ The State Defendants on one hand argue that Curling Plaintiffs' pollbook/PollPad arguments fall outside the bounds of this case as not properly pled in the operative complaints. The Court has already "addressed and rejected" this argument, (*See* 9/28/20 Paper Backup PI Order, Doc. 918 at 4), and need not further address it here. On the flipside, the Coalition Plaintiffs argue that the State Defendants have not addressed this "claim" in moving for summary judgment. But there is no separate PollPad/pollbook "claim," in this case. The Coalition Plaintiffs' pollbook arguments are raised as a component of their substantive constitutional claims (Counts I and II). The State Defendants clearly moved for summary judgment in full as to both claims.

backups have to be printed and distributed, they do not contain fully up-to-date information come Election Day.

In light of this problem, the Coalition Plaintiffs, at the preliminary injunction stage, sought to require the State Defendants to push back the print date for the paper backup lists so that the paper lists would include more up-to-date information. After a hearing and the presentation of evidence, the Court granted the Coalition Plaintiffs' request for injunctive relief and ordered, among other things, that the State provide updated paper backups at a later date. (*See* Doc. 918 at 64–67.) On appeal, the Eleventh Circuit vacated the preliminary injunction. *Curling*, 50 F.4th at 1125. In particular, the Circuit Court concluded that the Coalition Plaintiffs failed to demonstrate “a severe burden on the right to vote attributable to the State’s print date for the paper backup,” and that, on the other side of the scales, “relevant and legitimate state interests” justified the State’s existing hard copy print date. *Id.* (citing “administrative factors—the need to distribute a large number of lengthy lists while also managing other preparation tasks in advance of Election Day”).

Now, at summary judgment, the Coalition Plaintiffs rely, first, on the same evidence that the Eleventh Circuit found insufficient to establish a burden that outweighed the State’s administrative interests. In addition, the Coalition Plaintiffs argue that new evidence supports the grant of relief here. In briefing, the Coalition states, without citation, that “[t]he State Defendants do not update and distribute paper pollbook back-ups when critically needed in runoff elections.” (Coalition

Pls.’ Resp., Doc. 1624 at 77.) They also cite to new evidence that the PollPads are connected to the internet. (*Id.*) (citing Lenberg’s Dep Doc 1613 p. 72) (explaining that, while at the Coffee County Elections Office, Ms. Hampton “showed me that it was connected to the internet during its operation and that they literally could go order Domino’s Pizza and have it delivered while it was connected to the internet.”) So, according to the Coalition, the PollPads are subject to the same cybersecurity risks as the rest of the electronic voting machinery.

The Court will not rehash a request for a remedy that the Eleventh Circuit has already expressly disapproved as not justified or sufficiently tied to the voting problems identified. *Curling*, 50 F.4th at 1123 (noting that “delays or wait times at the polling places” were not sufficiently related to the fact that the State’s paper backups were not up to date). Indeed, as the Court of Appeals noted the nature of the curative remedy requested (i.e., the later provision of the voting information) was distinctively administrative in character and challenged issues within the discretion of the Secretary of State’s Office. But, to the extent the Coalition Plaintiffs challenge the PollPads as a coordinated part of Georgia’s electronic voting system — regardless of whether or not the Election Assistance Commission (“EAC”) certification technically covers the PollPads (*see* Defs. MSJ, Doc. 1568-1 at 6) — the operation of the PollPads (or other similar devices used in their place) remains relevant to the functioning, integrity, and reliability of the election system challenged in this case. Evidence of this nature is plainly relevant here and can be

presented at trial. The Court, however, will not allow the Coalition Plaintiffs to wander into remedy turf not directly relevant to the central issues in this case.

VI. Conclusion

The importance of the security, reliability, and functionality of state election systems, classified by the U.S. Homeland Security Department as critical national infrastructure, cannot be overstated in a world where cybersecurity challenges have exponentially increased in the last decade. The dynamics of how a breach in one part of a cyber system may potentially carry cybersecurity reverberations for the entire system for years to come exemplifies the important concerns raised in this case. The constitutional voting claims raised here involve complex evidence, legal issues, and events, heated by the political stresses of the era. Still, the Court reminds the reader that the fact that this Order allows Plaintiffs' constitutional claims to proceed to trial, with some exceptions, simply means that there are sufficient factual disputes underlying the legal disputes here to require a trial. But, as stated at the outset of this long Order, collaborative efforts to address the issues raised in this case might be more productive for the public good.

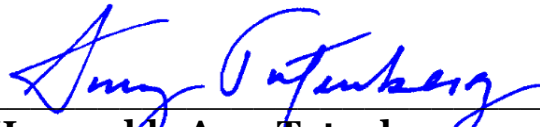
For the reasons articulated above, the State Defendants' Motions for Summary Judgment [Docs. 1567, 1568] are **GRANTED IN PART AND DENIED IN PART**. The motions are granted as to Plaintiffs' DRE claims (Counts I and II of both Third Amended Complaints) but denied as to the substantive BMD claims (Counts III and IV of the Curling Plaintiffs' Third Amended Complaint and Counts I and II of the Coalition Plaintiffs' Supplemental Amended Complaint).

Under the umbrella of the substantive BMD claims, the Coalition Plaintiffs' collateral theories and relief requests — related to ballot secrecy, scanner settings, and paper backups of pollbook information — are, for the most part, outside the scope of this case, with the following express qualification:⁷⁹ evidence regarding the functioning of the pollbooks and PollPads,⁸⁰ in connection with the operation of the election system as a whole, is still relevant, as discussed in Section V.D.4.

Additionally, as discussed herein, because the Plaintiffs' asserted harm is not traceable to Fulton County, Fulton County's Motion for Summary Judgment [Doc. 1571] is **GRANTED IN FULL**.

Trial is set for **January 9, 2023**. The current pretrial schedule is outlined the Court's Order of October 13, 2023. (Doc. 1700.)

IT IS SO ORDERED this 10th day of November, 2023.



Honorable Amy Totenberg
United States District Judge

⁷⁹ The Coalition Plaintiffs, however, may continue to pursue those remedies — related to ballot secrecy, scanner settings, and pollbook paper backups — via state administrative or judicial avenues, as discussed in Section V.D.

⁸⁰ Similarly, evidence regarding any device performing the same or similar functions that Defendants may deploy in place of, or as a supplement to, the pollbooks/PollPads is also relevant to the issues at hand.